Paperback

How a modern and secure workplace can help your organization become relevant

wortell

Jasper Bernaers

Paperback

How a modern and secure workplace can help your organization become relevant

Jasper Bernaers
CTO, Wortell Belgium

wortell

Table of contents

1.
Introduction.

1. Introduction.

Hi there!

First of all, thank you so much for reading my first E-book.

Over the past few years, I've been actively engaged with a lot of customers and communities in Belgium. I've had the opportunity to interact with customers on a daily basis focusing on projects and managed Microsoft 365, Microsoft Azure, and Microsoft Security services.

As a passionate IT professional, I'm always interested in finding out how I can best help our customers. I'm curious to know how people think technology can most benefit their organizations. Sometimes they require a high level of agility, distributed teams, ownership, and a drive for modern IT. Other times, they need a strict top-down IT organization and more stability or maturity to help their customers drive business.

My main role has been to provide action plans and advice on modernization to cloud-first technology. I've been activity engaged in delivering migration myself – yes, I believe I should understand technology in general to have realistic conversations about it. I've also worked as an internal system engineer, a position in which I was responsible for infrastructure, servers, domain controllers, and identity management — together with integrators, partners, and colleagues.

My motivation for writing this e-book is to bring up the conversation about a digital workplace. I love every organization with a vision and an ambition to drive effectiveness and productivity in a very conscious way.

In my career, I have always tried my best to create solutions in a 'standard' way. In our implementation teams, we re-use many of our standard solutions for customers that require the same building blocks. Standardization has created effectiveness, which you definitely need if you want to move fast.

Thank you so much for reading. If you have any questions, you can find me on Twitter or LinkedIn.

Jasper Bernaers
CTO, Wortell Belgium

2. Digitalization: an ambition.

2. Digitalization: an ambition.

Welcome to 2022. The world has changed since the start of the COVID-19 pandemic. Organizations struggle to better anticipate on their workforce so they can provide help and achieve their organizational ambition.

To improve collaboration and connect with each other in new ways, a more modern approach is necessary — things should be done differently. I don't want to elaborate too much on the fact that it's becoming a huge challenge for CIOs and IT managers since the world has shifted into this new digital era.

Working differently has become a new standard. And the change driver is coming from the outside. Covid-19 has pushed global organization in permanent remote-work. But also, mid-size organization are aware of the effectiveness of remote working and are creating methods and environment to elaborate on this new era of working different. This change is happening as we speak — not accepting these facts and new signals from different markets and sectors simply isn't an option. From my opinion, It isn't possible not to change anymore.

To be relevant new trends are showing op as for example, in a more economically driven and climate aware world, I believe digitalization is one of the core ambitions of every organization. And digitalization can help create an environment that includes and impacts other global world discussions are we are seeing today.

It can really help to connect people from within your organization. And I'm sure people should come first. On the other hand, I'm convinced that they all need the right support and digital platforms to make the most of their jobs and feel connected, empowered, and supported.

I have mapped the challenges I believe are important defining factors for successful technological adaptation in today's world. I will elaborate on these topics throughout this e-book. The main challenges are:

- To connect people so they can collaborate in a different way with new technical possibilities, keeping in mind the experience needs to be great. It should be simple, transparent, and team driven. There's no room for individuality.
- To use proven standards that do work. Standards are used in various organizations and experts are activity building best-practices so we should trust standards more. Slowness of not using standards or not believing them is sometimes killing organizations from within. This results in slow implemen-

tation speed, which leads to a lack of confidence and, therefore, less relevance.

- To provide the right tools that work for organizations in a modern world — where physical locations don't impose any limitations — with the same security level as in the early on-premise days, when everything was stable and properly (or better) protected.
- To be fast enough and accelerate your business goals. Timing is everything. A lack of speed equals a lack of relevance.
- To get you security maturity up to par by improving it and growing into a workplace that is more secure in terms of technology. This is more important than ever.

Companies are forced to work differently than before. Those who are the most adaptable will survive.

> “Employees want the best of both worlds: over 70 percent of workers want flexible remote work options to continue, while over 65 percent are craving more in-person time with their teams. To prepare, 66 percent of business decision makers are considering redesigning physical spaces to better accommodate hybrid work environments.” [1]

I firmly believe that extreme flexibility and hybrid work models will define the post-pandemic workplace. The COVID-19 outbreak was a driver for overall change within organizations. And even though we hope that COVID-19 will soon be a distant memory, the challenge of unlocking hybrid working will remain.

[1] https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work

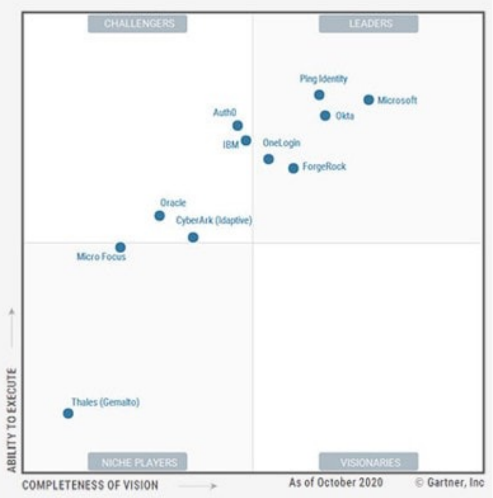
3. Where do you choose to go?

3. Where do you choose to go?

3.1 Gartner Magic Quadrants

Defining which technology comes first and how to implement it is an organizational choice. I'm confident Microsoft brings the best to each organization, so I believe it's the go-to choice. What about you?

Microsoft is listed as a leading solution provider in the Gartner MQ for Access Management because of its technical capability and vision. Additionally, you can find Microsoft under 'Endpoint Management,' 'Cloud Access Security Brokers,' 'Information Archiving,' and 'SIEM.' These multiple positions (most of which are in the leader's quadrant) prove that the platform approach and strategy to integrate and interconnect solutions work, providing a more business-oriented answer to customers' digitalization challenges.



If you choose the right platform or define strategically which platform you'll use, I believe it facilitates and speeds up digitalization.

Microsoft Security is a leader in five Magic Quadrants[2].

[2] https://www.microsoft.com/en-us/security/business/security-leaders-gartner-magic-quadrant

3.2 You are a Microsoft-first organization

Since Steve Balmer quit as a CEO and passed the baton to Satya Nadella, Microsoft has become a different company. With the ambition to empower each and every person to achieve more, Microsoft has embraced real change in the (digital) world.

Its ambition was not focused on the big numbers and segmented solutions. Satya's vision is to bring all people and solutions together in one cloud-connected world. Not driven by their own agenda but integrated with their competitors, integrators, and partners — like it should be. This way, Microsoft really wants to help its customers. And as organizations don't use Microsoft technology alone, it has become a great success — with a high increase in market share.

Consider Microsoft as a platform. Microsoft delivers two main solutions: a platform where you can collaborate (Microsoft 365) and a platform that can host almost any system or service in the Cloud (Microsoft Azure).

Questions. Are you running Windows machines, using Exchange Online for email and SharePoint, Teams or OneDrive for collaboration? Have you already become a Microsoft-first organization?

3.3 Why use Microsoft 365 for collaboration?

The three main collaboration solutions are Microsoft 365, Google Workspace, and Slack. Generally speaking, they are the same. Each aims to allow people to connect, collaborate, chat, meet, and share data. So, why use Microsoft 365 for collaboration? Mainly because it offers integration into a single platform. If you use Microsoft 365, all your company data is integrated into one system. It's easier to protect and manage, and all alerts and risks are in one place.

When it comes to company data, there are two places where nearly all-important data is located: on your servers, in your applications, and in your company systems (datacenter) and in Microsoft 365 in the other.

My question for you is, how much data is in Microsoft 365 right now? How much data is under your organizational control?

3.4 Microsoft Azure for your datacenter

Perhaps this title pushed your buttons because you believe Azure is no place to host 'traditional' servers. And yet I'm pitching the idea to you. Think about it for a moment and ask yourself, 'Why not?' Is it worse than your private, distributed, or cloud datacenter?

Azure can help your organization bring everything into the Microsoft Platform. Here's why you should want this: you'll have everything consolidated and collected in one place so you can increase your security maturity. Focus on the Microsoft platform and build expertise using one vendor's solution.

Azure can leverage solutions as a service and therefore much better than infrastructure as a service. But it's still powerful when it comes to single platform focus and security insights and risk management.
When it comes to features and capabilities, there are lots of things I could discuss. But in this context, I just want to clarify the roadmap or solution set you can use to move your services to the cloud.

3.5 What if you don't use Microsoft M365 with embedded Security mechanism?

Each organization is having a lot of documents and real-time communication in Microsoft 365. Your Microsoft servers are running somewhere in a data-center on-premise or in the cloud. Perhaps in Azure — so the security question here is: why you would still put a non-cloud-oriented solution in between for protection of these systems.

Question. Are you capable of measuring, controlling, and responding to alerts in your main collaboration, services, and server solutions? Does your security model still cover all aspects of the broader workplace? I really don't believe we should get rid of on-premises, application, and network security solutions. I just want to ask if it's common that more data services are shifting to the public cloud.

So, let's consider the situation together. If almost all essentials business critical solutions are hosted in Microsoft 365 and Azure (which is the case), do you still believe you shouldn't use Microsoft's security solutions?

Here's my opinion: Microsoft hasn't had the best reputation when it comes to secure systems *in the past*. Now, things have changed as a result of billion dollar investments, acquisitions, and other aspects. Microsoft's cloud native and cloud focused solutions can leverage so much at such a fast pace that using them — instead of more complex solutions — can be a strategic or tactical decision.

Trusting one vendor with everything is a major, bold choice to make for your organization. I think that clarity of products and services can help to write up your organizations ambition to choose Microsoft-first so you could bring your people in the same direction.

And it's always possible for disaster recovery (DR) to work with multi-geo. Or you can choose another platform that allows for a 'back-up' of your environment.

3.6 Microsoft and security, confidentiality, and compliance

The security of your Microsoft cloud service is a partnership between you and Microsoft.

The cloud is not just a space — it's a model.

Microsoft is committed to working on its Trust principles[3] that are running the Microsoft cloud business. These four defined principles are: security, privacy, transparency, and compliance. It's a lot to explain. I've summed up the most important takeaways per topic below.

Security

- Microsoft has over 100 datacenters with a cutting-edge operational security team that has restricted access to its own systems, leverages 24/7 monitoring, and provides global security experts.

[3] https://www.microsoft.com/en-us/trust-center/privacy

- Microsoft has invested 1 billion dollars a year in cybersecurity.
- 3500+ security professionals analyze more than 6.5 trillion signals a day.
- 5 billion malware threats per month are stopped by Microsoft.
- DCU programs include Tech Support Fraud, Online Child Exploitation, Global Strategic Enforcement, Cloud Crime, and Malware Nation-State Actors.
- Cyber Threat Intelligence Program (CTIP)[4]
- Microsoft is focusing on the 'Assume Compromise' strategy, which allowed a different view of the security landscape than years ago.

Read more about Microsoft's Security Foundation[5] on a global scale.

Privacy

"We will ensure your data is Secure" — Brad Smith, President and Chief Legal Officer

Microsoft is committed to:

- Using the GDPR as a catalyst for broader efforts to improve data handling globally.
- Building privacy into its services as part of the Microsoft Security Development Cycle[6].

[4] https://docs.microsoft.com/en-us/security/gsp/informationsharingandexchange
[5] https://azure.microsoft.com/en-us/overview/security/
[6] https://www.microsoft.com/en-us/securityengineering/sdl

Customers stay in full control

- Microsoft administrators cannot access customer data. Support engineers need to get explicit customer approval to access data stored in the customer's tenant. Customer Lockbox inserts customers into the approval workflow.
- Data residency is transparent and compliant. Microsoft contractually adheres to data residency requirements by jurisdiction and provides customers insight into where their data is stored.
- Microsoft routes all government requests for data access to their customers[7].
- Microsoft is committed to maintaining customer privacy and has extended our GDPR data subject rights to all customers worldwide.

Transparency

Microsoft delivers:

- Geographical locations where customer data is located.
- Visibility into how it handles customer data, how it protect this data, and how it is in control.
- Publication of legal requirements for customer data placed on Microsoft by law enforcement agencies.

Compliance

Microsoft's compliance and regulation[8] can be found at: https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

[7] https://blogs.microsoft.com/datalaw/our-practices/

[8] https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

4. Technical modern workplace implementation.

4. Technical modern workplace implementation.

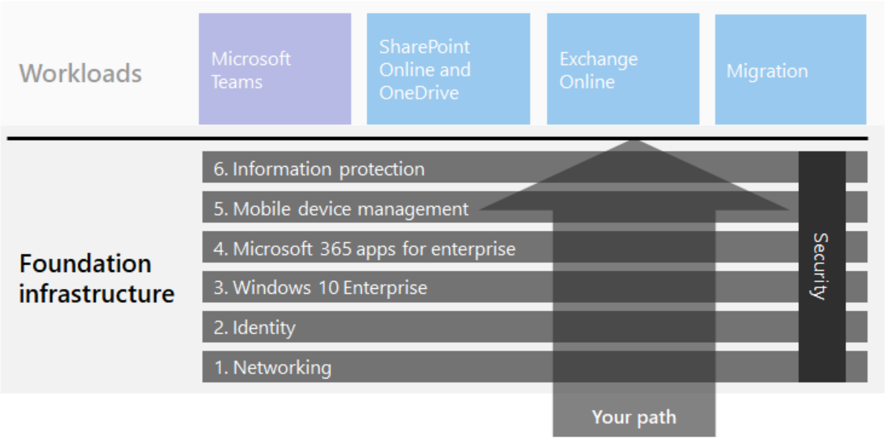
What daily conversations have taught me is that most of the time, we decide to take on IT projects when there is a big need for change — for example, when there's a problem, or cost optimization is possible we create an IT-project.

IT-projects without a vision and strategy narrows the broader conversation of creating a digital and secure workplace.

During these conversations, we often talk about an opportunistic approach, which may include the migration of documents, Exchange, or infrastructure to Azure. I believe we should create more ambitious roadmaps and modernization tracks *throughout* the organization – which requires a technological transformation.

If you are willing to move to Microsoft 365 at full throttle, my short advice is to get the most out of the solution set available.

I'm a great fan of the Microsoft Foundation Infrastructure, as it provides guidance on where to start. Have you started using Microsoft Teams in response to the COVID-19 crisis? There's nothing wrong with that. But now it's time to ensure a higher level of security and structure in the future digital workplace.


Workloads
Microsoft Teams
SharePoint Online and OneDrive
Exchange Online
Migration
Foundation infrastructure
6. Information protection
5. Mobile device management
4. Microsoft 365 apps for enterprise
3. Windows 10 Enterprise
2. Identity
1. Networking
Security
Your path

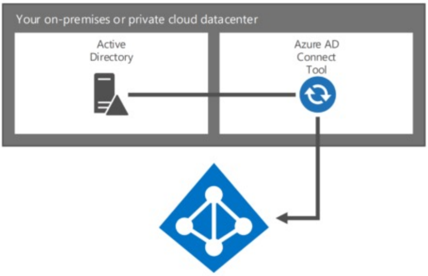
4.1 Start with identity management and extend Active Directory to Azure AD

Identities are digital personalities that allow you to 'log on' to nearly every organizational service to authenticate in a secure way. Some consider identity management as a separate product that is included in all Microsoft solutions. But let me tell you this: virtually every organization I know uses its Active Directory as its primary identity solution. And these organizations are fully focusing into one Identity platform.

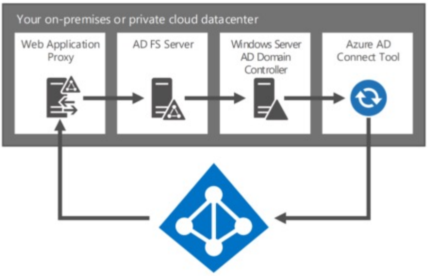
Did you know that Microsoft Azure Active Directory is also a "Leader" in the Gartner Magic Quadrant for Access Management[9]?

[9] https://www.microsoft.com/security/blog/2020/11/24/microsoft-azure-active-directory-again-a-leader-in-gartner-magic-quadrant-for-access-management/

Install Azure AD Connect and sync your users and groups to Azure AD.



Directory and password synchronization



Federation

Your on-premises or private cloud datacenter
Web Application Proxy
AD FS Server
Windows Server AD Domain Controller
Azure AD Connect Tool

You can use directory and password synchronization to move all identities from your current environment to Azure AD. I prefer starting with the hybrid scenario and implementing the full cloud scenario later. Worst-case ADDS in Azure: to have the 'controls' transformed to the primary Directory in Azure AD. Azure AD DS integrates with your existing Azure AD tenant. This integration lets users sign into services and applications connected to the managed domain using their existing credentials. You can also use existing groups and user accounts to secure access to resources. These features provide a smoother lift-and-shift of on-premises resources to Azure.

Why? Microsoft Azure AD is beyond the current 'legacy' integration and is a next-gen identity platform. Make it simple. If you don't need third-party solutions (which always limits new capabilities) don't go for it. Use native Azure AD. Also it's a big opportunity to leave things behind and smoothly shift to ADDS or Azure AD. One platform = one attack-surface. It could be easier to manage and protect.

4.2 Migrate your Exchange workload with Exchange Hybrid Wizard

You can move your mailboxes (Exchange) to Microsoft 365 to have them hosted in a software-as-a-service model. What you need to do is set up Azure AD Connect to synchronize all identities to Azure AD / Microsoft 365.

It's best to change users' UserPrincipalName (UPNs) — if required — as well as their e-mail addresses. I think it's easier for end users to have the same logon everywhere.

From the technical perspective, you could pre-sync all mailboxes to a state of 95%. This move of the mailbox is throttled and doesn't really impact your network bandwidth. If it's problematic, you can configure your virtual web services in bandwidth or synchronization jobs.

To properly do a cutover migration, it is best practice to migrate about 2,000-5,000 mailboxes in cutover scenario. A cutover migration means that every mailbox will be migrated at the same time and takes away the hybrid challenges for calendar sharing and access to resources.

After a hybrid Exchange migration, it's time to move the email relay to Microsoft 365. Or you can work with alternative solutions. I prefer to make it as simple as possible. Don't create complexity regarding hybrid mail flow. You can keep hybrid Exchange in the first phase with operational management to AD and Exchange Online.

4.3 Migrate personal data to OneDrive

Document data is one of the most important things in any workplace. It's crucial to take personal data into account when migrating. It will help support the shift to Microsoft 365. When you help people to have a great usability working on their documents, they will be more engaged to use the 'corporate solutions' above limited consumer versions of Microsoft 365.

You could use 'OneDrive Known Folder move' to automatically discover your favorites, desktop document and place them on end-user's OneDrive for Business. In my experience, people love this feature. It's easy to implement, and it has additional value without changing what's at the core of working on personal documents. At first, we were hesitant about activating this feature for the entire organization. Now, it's part of our standardized workplace approach. This feature has no disadvantages — only great features to remove old file shares and use new capabilities such as site restore, file restore in SharePoint.

A second option for migration might be migration of your home drives — a capability that provides more control. My advice is to devise a simple, comprehensible communication plan.

4.4 Migrate departments to Teams or SharePoint Online

I'm not going deep into details for document migration. But I will provide the high-level strategy and migration tips to bring documents to Microsoft 365.

First step; **Assess** your current environment and understand the needs of your organization. It's not a technical approach. You could ask opinions and ask for best practices that employees are currently using to collaborate on documents. Hosting panels and asking feedback is the most important tip to do a smooth migration. When doing polls or a survey you give people the opportunity to come up with business scenarios and you give them the chance to be heard.

For the technical perspective you should investigate usage metrics and understand the current file-structures how your company is working with folders, SharePoint or different document systems.

Then, **migration** of team data could result in Microsoft Teams Libraries and organization data could land in SharePoint Online. **Personal data** (only actively in use by 1 person) **should** land in **OneDrive**.

There are great tools on the market to do this technical assessment. A phased approach is necessary. **Standards** & **building blocks** will help with the speed of implementation. My main advice: clear **communication** and **training** are well recommended!

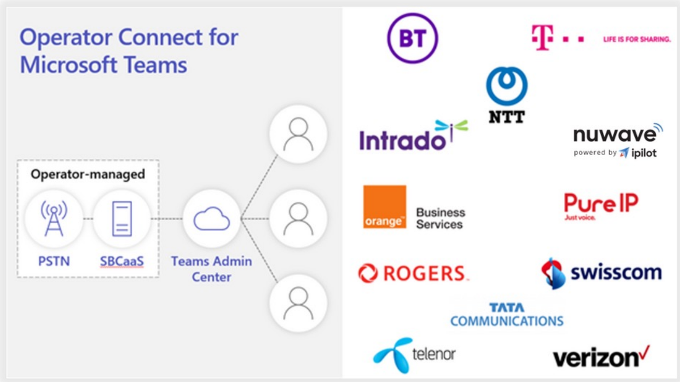
4.5 Voice shift from on-premises to Microsoft 365 or any other cloud integration solution

There are 5 options of the Microsoft Teams voice solution:

1. Phone system with Microsoft's calling plan. This is a full Microsoft solution that is hosting numbers for organizations. With a fixed cost per minute, you are able to make phone calls without having to host infrastructure or maintain the telephony platform.
2. Phone system with your own carrier, direct-routing, shared SBC (Session Border Controller) are options. You could use your SBC system and route it towards Microsoft 365 to pick-up the phone in Microsoft Teams. Great capabilities.
3. Phone system with own carrier via Skype for Business or Cloud Connector Edition. Here you can still use your previous Skype for Business system to integrate and migrate the connections towards Microsoft Teams. Don't forget, Skype for business online is end-of-life on 31/07/2021[10]. Skype on-premise will stick around for some time.

[10] https://techcommunity.microsoft.com/t5/healthcare-and-life-sciences/skype-for-business-online-end-of-life-july-31-2021/ba-p/779137

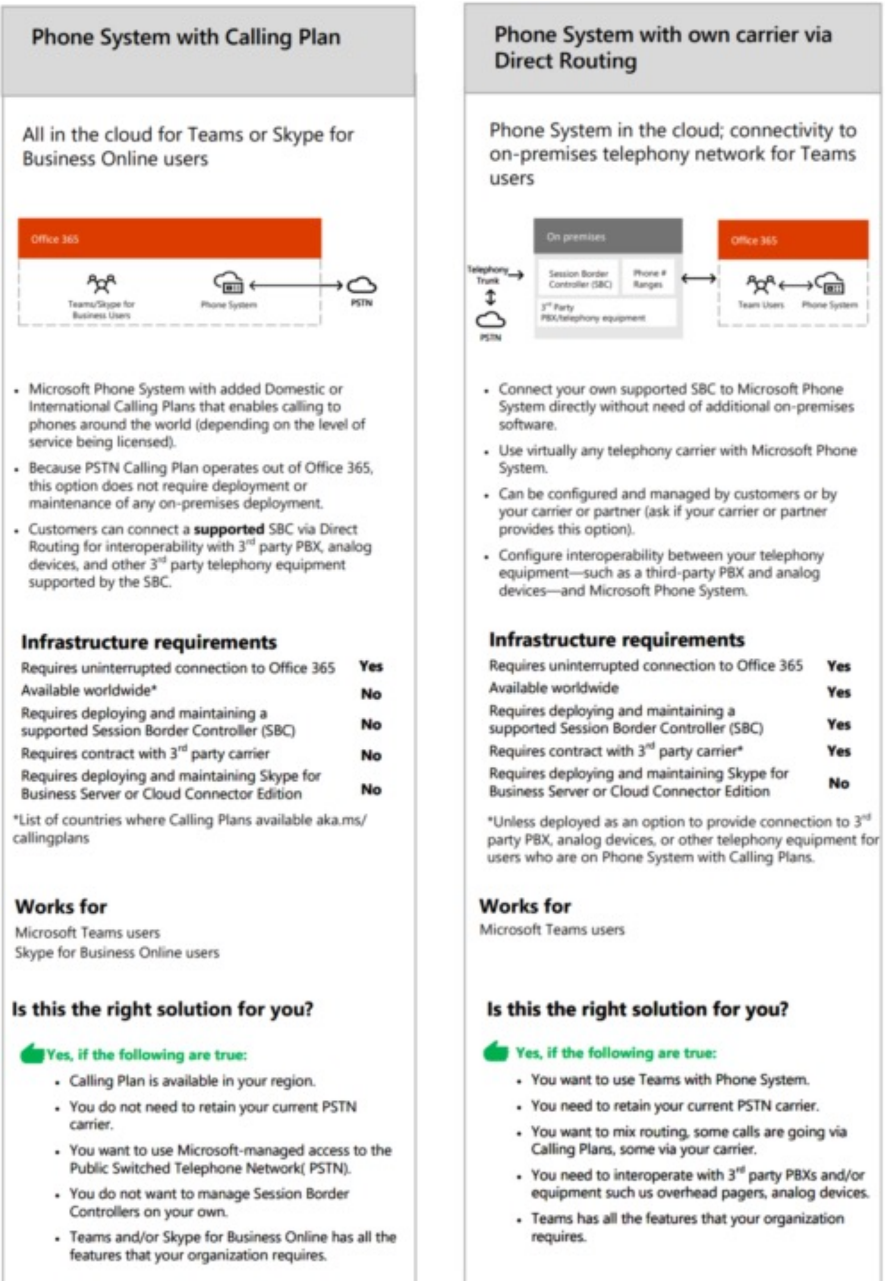
4. Enterprise voice in Skype for Business with own carrier.
5. New: Operator Connect is keeping your preferred operator and contracts, while enabling a modern calling experience in Teams. More info: here[11].



Don’t go for less. Use Microsoft Teams. And if you will choose other platforms or solutions think about the adoption impact. People need time to learn new technology and Microsoft software is changing continuously. Do you still want to bring multiple solutions to solve the same challenge? Think about the speed of implementation compared to the easiness of one platform for your workers.

There are solutions on the market to help shift to cloud voice with Microsoft Teams. But keep in mind that Microsoft shifted their own organization to Teams.

[11] https://techcommunity.microsoft.com/t5/microsoft-teams-blog/introducing-operator-connect-and-more-teams-calling-updates/ba-p/2176398



Phone System with Calling Plan

All in the cloud for Teams or Skype for Business Online users

Office 365
Teams/Skype for Business Users
Phone System
PSTN

- Microsoft Phone System with added Domestic or International Calling Plans that enables calling to phones around the world (depending on the level of service being licensed).
- Because PSTN Calling Plan operates out of Office 365, this option does not require deployment or maintenance of any on-premises deployment.
- Customers can connect a **supported** SBC via Direct Routing for interoperability with 3rd party PBX, analog devices, and other 3rd party telephony equipment supported by the SBC.

Infrastructure requirements

Requires uninterrupted connection to Office 365	**Yes**
Available worldwide*	**No**
Requires deploying and maintaining a supported Session Border Controller (SBC)	**No**
Requires contract with 3rd party carrier	**No**
Requires deploying and maintaining Skype for Business Server or Cloud Connector Edition	**No**

*List of countries where Calling Plans available aka.ms/ callingplans

Works for

Microsoft Teams users
Skype for Business Online users

Is this the right solution for you?

Yes, if the following are true:

- Calling Plan is available in your region.
- You do not need to retain your current PSTN carrier.
- You want to use Microsoft-managed access to the Public Switched Telephone Network(PSTN).
- You do not want to manage Session Border Controllers on your own.
- Teams and/or Skype for Business Online has all the features that your organization requires.

Phone System with own carrier via Direct Routing

Phone System in the cloud; connectivity to on-premises telephony network for Teams users

- Connect your own supported SBC to Microsoft Phone System directly without need of additional on-premises software.
- Use virtually any telephony carrier with Microsoft Phone System.
- Can be configured and managed by customers or by your carrier or partner (ask if your carrier or partner provides this option).
- Configure interoperability between your telephony equipment—such as a third-party PBX and analog devices—and Microsoft Phone System.

Infrastructure requirements

Requires uninterrupted connection to Office 365	**Yes**
Available worldwide	**Yes**
Requires deploying and maintaining a supported Session Border Controller (SBC)	**Yes**
Requires contract with 3rd party carrier*	**Yes**
Requires deploying and maintaining Skype for Business Server or Cloud Connector Edition	**No**

*Unless deployed as an option to provide connection to 3rd party PBX, analog devices, or other telephony equipment for users who are on Phone System with Calling Plans.

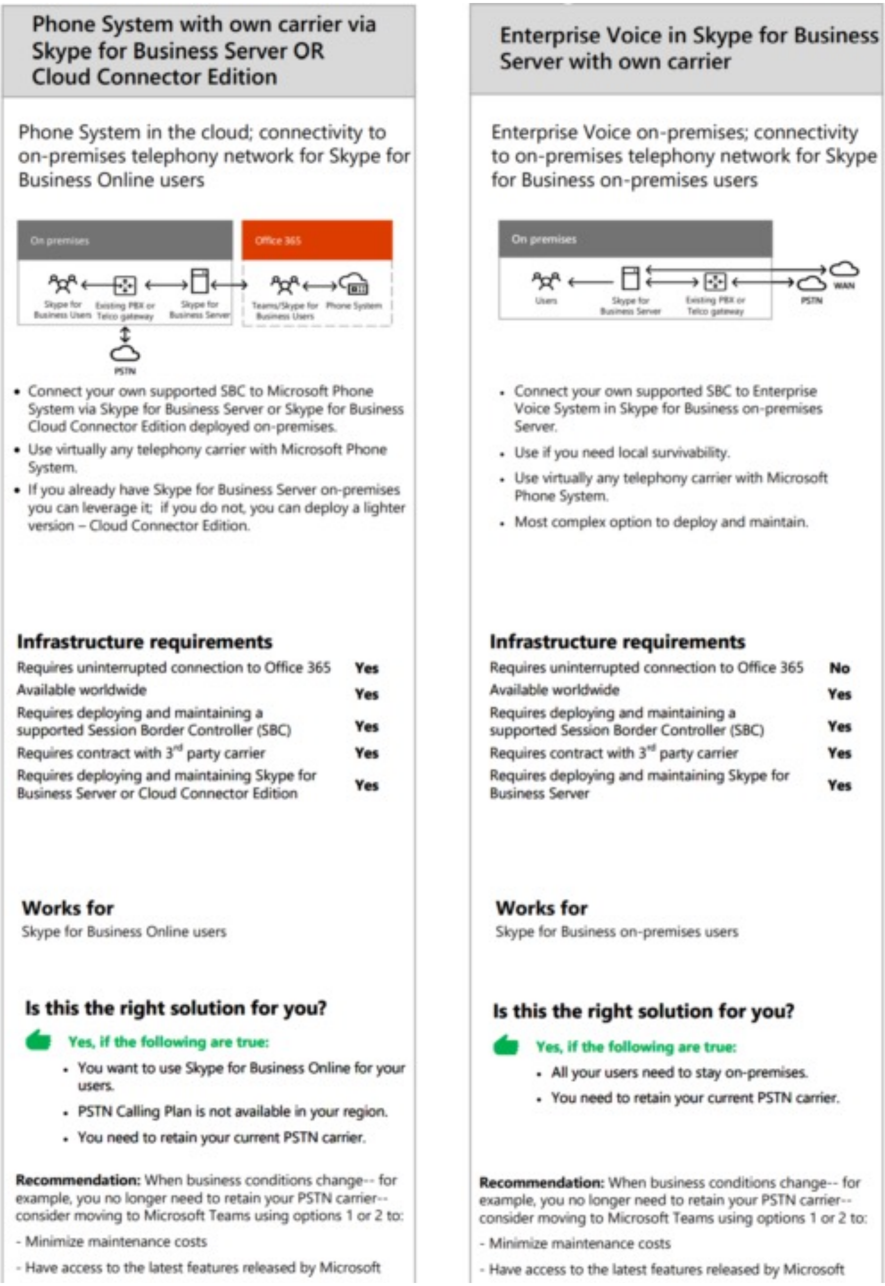
Works for

Microsoft Teams users

Is this the right solution for you?

Yes, if the following are true:

- You want to use Teams with Phone System.
- You need to retain your current PSTN carrier.
- You want to mix routing, some calls are going via Calling Plans, some via your carrier.
- You need to interoperate with 3rd party PBXs and/or equipment such us overhead pagers, analog devices.
- Teams has all the features that your organization requires.



Phone System with own carrier via Skype for Business Server OR Cloud Connector Edition

Phone System in the cloud; connectivity to on-premises telephony network for Skype for Business Online users

On premises
Office 365
Skype for Business Users
Existing PBX or Telco gateway
Skype for Business Server
Teams/Skype for Business Users
Phone System
PSTN

- Connect your own supported SBC to Microsoft Phone System via Skype for Business Server or Skype for Business Cloud Connector Edition deployed on-premises.
- Use virtually any telephony carrier with Microsoft Phone System.
- If you already have Skype for Business Server on-premises you can leverage it; if you do not, you can deploy a lighter version – Cloud Connector Edition.

Infrastructure requirements

Requires uninterrupted connection to Office 365	Yes
Available worldwide	Yes
Requires deploying and maintaining a supported Session Border Controller (SBC)	Yes
Requires contract with 3rd party carrier	Yes
Requires deploying and maintaining Skype for Business Server or Cloud Connector Edition	Yes

Works for

Skype for Business Online users

Is this the right solution for you?

Yes, if the following are true:

- You want to use Skype for Business Online for your users.
- PSTN Calling Plan is not available in your region.
- You need to retain your current PSTN carrier.

Recommendation: When business conditions change-- for example, you no longer need to retain your PSTN carrier-- consider moving to Microsoft Teams using options 1 or 2 to:

- Minimize maintenance costs

- Have access to the latest features released by Microsoft

Enterprise Voice in Skype for Business Server with own carrier

Enterprise Voice on-premises; connectivity to on-premises telephony network for Skype for Business on-premises users

- Connect your own supported SBC to Enterprise Voice System in Skype for Business on-premises Server.
- Use if you need local survivability.
- Use virtually any telephony carrier with Microsoft Phone System.
- Most complex option to deploy and maintain.

Infrastructure requirements

Requires uninterrupted connection to Office 365	No
Available worldwide	Yes
Requires deploying and maintaining a supported Session Border Controller (SBC)	Yes
Requires contract with 3rd party carrier	Yes
Requires deploying and maintaining Skype for Business Server	Yes

Works for

Skype for Business on-premises users

Is this the right solution for you?

Yes, if the following are true:

- All your users need to stay on-premises.
- You need to retain your current PSTN carrier.

Recommendation: When business conditions change-- for example, you no longer need to retain your PSTN carrier-- consider moving to Microsoft Teams using options 1 or 2 to:

- Minimize maintenance costs

- Have access to the latest features released by Microsoft

I mean, they have a complex organization and multiple flavors of requirements and needs. They have call centers everywhere in the world and have hierarchic organizations matrixes for the chain in command.

Tip: Don't build a complex integration for the 5% that had needs different functionality as it doesn't help your customers. Small changes with simplifications can create less complexity and more agility.

4.6 Microsoft Endpoint Manager

Microsoft Endpoint manager is a great solution for managing all endpoints. From Windows 10, 11 till iOS or Android.

To implement Microsoft Endpoint manager for Windows 10 or 11 you can easily onboard all current devices by doing 'Hybrid Join" or 'full cloud join' (azure AD only). In the more modern world, Azure AD Join is the new thing. Because it no longer has dependencies in the on-premise Active Directory. No GPO's, DNS or other mechanisms from the old days.

I believe Microsoft is investing to disconnect the old domain controller integration because it's almost at its maximum technical limitations.

It's best to onboard all new devices with Windows Autopilot. It enables smooth onboarding and will allow to do remote reset without touching the device. (Zero-touch)

When using Windows Autopilot with Azure AD Join you also have the possibility to leave the devices somewhere connected to the internet when doing the initial staging. For Hybrid Join it needs to be line-of-sight with Active Directory.

Implement Mobile Application Management (MAM) for mobile at least. Manage all your company owned devices. Don't leave unmanaged or unknown devices behind. These are creating security risks.

Tip: When enabling MAM there is an option to activate a pin code. I've done this implementation 20 times in the last year. It's a great opportunity for less mature organizations because they now have some sort of awareness for security improvements. And its low-end to activate. Working perfect.

4.7 Increase basic identity Security

A shortlist of best practice Identity Security implementations.

Multi-Factor Authentication or Azure Security Defaults.

Multi Factor Authentication (MFA) is a way of providing authentication by using an additional factor. (Or several) Something someone KNOWs, such as a password or pin code. Something someone HAS such as a mobile phone, a 'fido2' hardware token. Something that someone IS such as their Biometrics: fingerprint or facial recognition. By using MFA, the risk of identity compromise decreases a lot.

Conditional Access for easier login's – and more security. Conditional access provides 'access' when a specific condition has been met. For example: If you have a trusted device, you don't need to re-authenticate each time you open a browser and can use single-sign-on in Microsoft 365. Or force MFA when opening your computer outside of Europe, on public WIFI's, etc.

Connect your devices to Azure AD with Endpoint Manager. "Cloud intelligence drives management" Endpoint manager is providing the capability to manage all devices from the Cloud. Connected devices can be well known and in control of your organization. This to comply with a default set of security standards.

SSPR or Self-Service Password Reset. The SSPR possibility Is an Azure Active Directory (AD) feature that enables users to reset their passwords without contacting IT staff for help. People can unblock their account themselves and continue working no matter where they are.

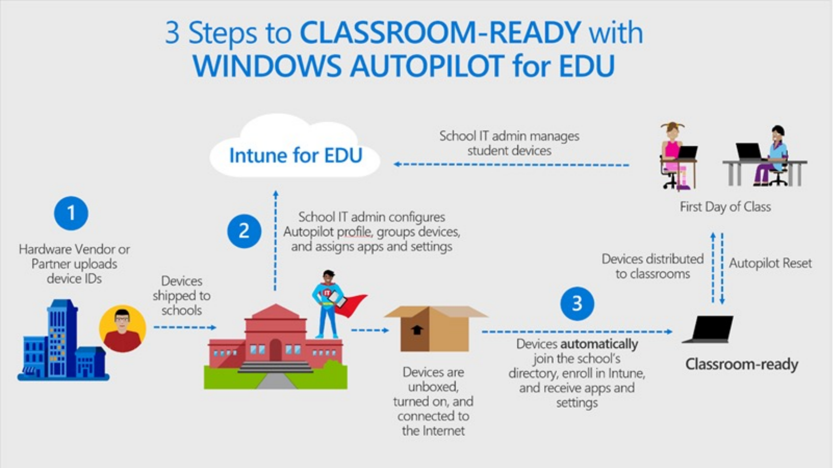
4.8 Windows Autopilot for enrollment of Windows devices

Scenario: In this picture you can see the 3 steps to make your classroom ready to deploy Windows 10 devices with Windows Autopilot.

1. When buying computers, vendors are able to provide a 'hardware hash' that can be automatically

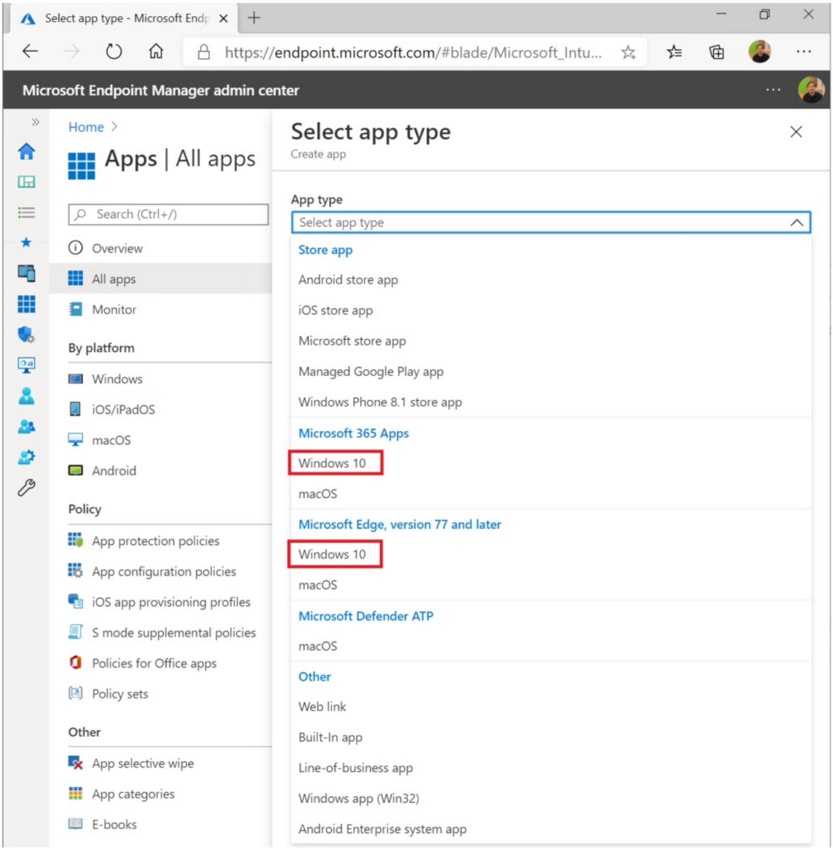
imported in Microsoft Endpoint Manager. These IDs are linked to devices in a customer tenant.

2. If ready the IT administration is able to assign this device to a group which applies policies or specific requirements for the student or employee.
3. The device will automatically join the school or corporate environment and will be ready to use without IT Interaction which is called zero-trust IT.


3 Steps to CLASSROOM-READY with
WINDOWS AUTOPILOT for EDU
Intune for EDU
School IT admin manages student devices
First Day of Class
1
Hardware Vendor or Partner uploads device IDs
Devices shipped to schools
2
School IT admin configures Autopilot profile, groups devices, and assigns apps and settings
Devices are unboxed, turned on, and connected to the Internet
3
Devices automatically join the school's directory, enroll in Intune, and receive apps and settings
Devices distributed to classrooms
Autopilot Reset
Classroom-ready

4.9 Software Deployment migration

Microsoft Office 365 ProPlus (now Microsoft 365 Apps) can be quickly deployed by Endpoint Manager. Microsoft Endpoint manager is delivering a built-in panel for easy and quick distribution for Office 365. There are 2 ways. You could work with the built-in configurator, or you could work with config.office.com -- This site helps IT administrators deploy, manage, monitor and secure Microsoft 365 apps within your organization.



Windows Updates can shift to Modern management as soon as possible when using Endpoint manager. Total control of windows Updates is built in. And rich insights are created in Microsoft Security Center. Which elevates control from on-premises to the integrated cloud.

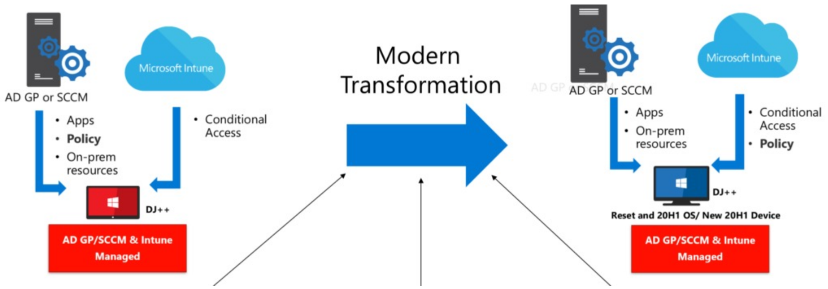
Microsoft Edge will deliver great value when it comes to browser support. Microsoft Edge can support old 'sessions' as well. It is: Azure AD integrated and super modern to use.

If needed you can integrate with Market solutions as Scappman, Patch My PC or Chocolatey for 'simple' deployable software. Next to online platforms you are also able to use own written scripts and create packages when necessary.

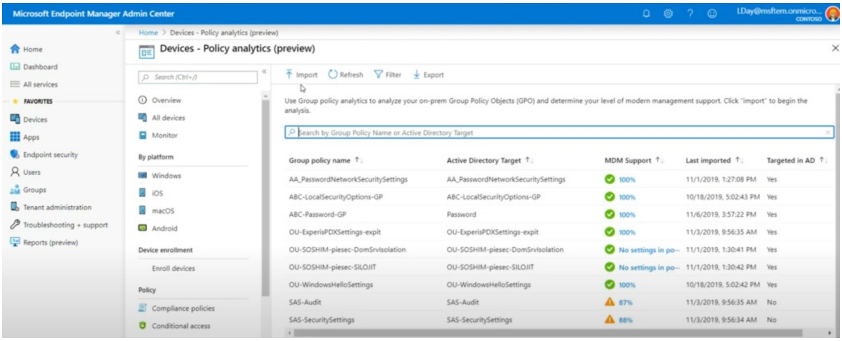
4.10 Group-Policy-Objects (GPO) Migration

Microsoft is currently working on policy analytics which will help the migration of GPO's to MDM policies with controls. But keep in mind, a lot of policies are used for legacy. I don't believe in migration of GPO's. I believe in a basis workplace 'greenfield' were you build standards for everyone. Not for groups. And if you do. For 10 groups. and 90% same architecture and flavors. So: Don't migrate non used GPO's. Rethink GPO's -> MDM policies. In a modern world protection or endpoints can be more important than setting IT-policies.

ADMX backed baselines will help for smooth and faster configuration. Whenever it's not possible use the OMA-URI's.



Most important try to be prepared for 80% to shift the authority from GPO's to MDM. And I would try to leave the GPO's in your on-premise DC's behind.



Devices - Policy analytics (preview)

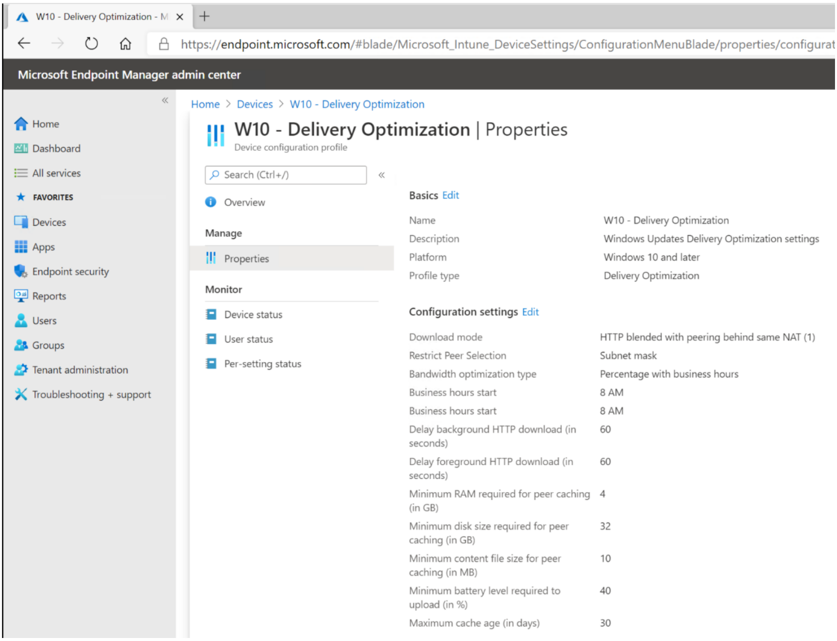
Use Group policy analytics to analyze your on-prem Group Policy Objects (GPO) and determine your level of modern management support. Click "import" to begin the analysis.

Group policy name	Active Directory Target	MDM Support	Last imported	Targeted in AD
AA_PasswordNetworkSecuritySettings	AA_PasswordNetworkSecuritySettings	✓ 100%	11/1/2019, 1:27:08 PM	Yes
ABC-LocalSecurityOptions-GP	ABC-LocalSecurityOptions-GP	✓ 100%	10/18/2019, 5:02:43 PM	Yes
ABC-Password-GP	Password	✓ 100%	11/6/2019, 3:57:22 PM	Yes
OU-ExperisPDXSettings-expit	OU-ExperisPDXSettings-expit	✓ 100%	11/3/2019, 9:56:35 AM	Yes
OU-SOSHIM-piesec-DomSrvIsolation	OU-SOSHIM-piesec-DomSrvIsolation	✓ No settings in po...	11/1/2019, 1:30:41 PM	Yes
OU-SOSHIM-piesec-SILOJIT	OU-SOSHIM-piesec-SILOJIT	✓ No settings in po...	11/1/2019, 1:30:42 PM	Yes
OU-WindowsHelloSettings	OU-WindowsHelloSettings	✓ 100%	10/18/2019, 5:02:42 PM	Yes
SAS-Audit	SAS-Audit	⚠ 87%	11/3/2019, 9:56:35 AM	No
SAS-SecuritySettings	SAS-SecuritySettings	⚠ 88%	11/3/2019, 9:56:34 AM	No

4.11 Windows updates improvements and tips

It's best practice to create a Windows 10 update ring with peer-to-peer caching that will not kill the internet break out of your organization. You can autonomously create segmented pre-test groups to validate the update version in production groups within the Windows update rings.

You can use the standard Security Baselines to implement the W10 MDM Baseline and MDATP configuration. Baselines are great for upgrading the maturity of your endpoints.


W10 - Delivery Optimization - M
https://endpoint.microsoft.com/#blade/Microsoft_Intune_DeviceSettings/ConfigurationMenuBlade/properties/configurat
Microsoft Endpoint Manager admin center
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices > W10 - Delivery Optimization
Search (Ctrl+/)
Overview
Manage
Properties
Monitor
Device status
User status
Per-setting status

W10 - Delivery Optimization | Properties

Device configuration profile

Basics Edit

Name	W10 - Delivery Optimization
Description	Windows Updates Delivery Optimization settings
Platform	Windows 10 and later
Profile type	Delivery Optimization

Configuration settings Edit

Download mode	HTTP blended with peering behind same NAT (1)
Restrict Peer Selection	Subnet mask
Bandwidth optimization type	Percentage with business hours
Business hours start	8 AM
Business hours start	8 AM
Delay background HTTP download (in seconds)	60
Delay foreground HTTP download (in seconds)	60
Minimum RAM required for peer caching (in GB)	4
Minimum disk size required for peer caching (in GB)	32
Minimum content file size for peer caching (in MB)	10
Minimum battery level required to upload (in %)	40
Maximum cache age (in days)	30

4.12 Shift infrastructure to Azure

Think about: **Rehost, Refactor, Rearchitect, rebuild, replace**!

If you want to do infrastructure shift, follow the next steps. Otherwise, you can do an assessment and write down all infrastructure and start with rearchitecting were possible. When you're hosting well known vendor applications try to get in touch and ask if they are planning for SaaS, Azure, others.

A 5 steps approach for moving infrastructure to Microsoft Azure.

1. Create an Azure Migrate project and add the Server Assessment solution to the project.
2. Set up the Azure Migrate appliance and start discovery of your server. To set up discovery, the server names or IP addresses are required. Each appliance supports discovery of 250 servers. You can set up more than one appliance if required.
3. Once you have successfully set up discovery, you can create an assessments and review the assessment reports.
4. Use the application dependency analysis features to create and refine server groups to phase your migration.
5. Migrate machines as physical servers to Azure.

Never forget: Rehost, Refactor, Rearchitect, rebuild, replace

4.13 Migration of legacy Active Directory Integration

If you wish to decommission legacy or old Active Directory infrastructure and are moving to Cloud Authentication with Microsoft Azure Domain Services or Azure Active Directory (AAD) you can systematically shift your used platforms to here.

In my experience it's not super problematic to shift application by application towards Azure Active Directory because your identity is known on-premises and in the Cloud and creates the trust in between. This means that the opportunity is there to smoothly move more and more applications towards Azure Active Directory without creating business impact. Some big platforms are even able to shift 1000 users in batches.

When more and more core applications are shifted to Azure Active Directory, you are able to monitor the active usage and you could try to implement extra security controls to prevent strange authentication behavior as passwords that are spread within the organization.

And yeah, sometimes there is an application which is just too old. That doesn't support the protocols of today. I would advise not to integrate and think in the long-term, strategic.

4.14 Build collaboration platforms with Microsoft Teams & SharePoint

Conclusions: I've probably missed some 'crucial' applications on-premises that are used for 20 years. I think that we need to leave complex legacy-systems behind. Choose SaaS solutions with future-benefits. Don't wait for phasing these out to go cloud. Do cloud and leave legacy behind. OR migrate and isolate. Built the new, migrate the old.

When it comes to a collaboration space I would:

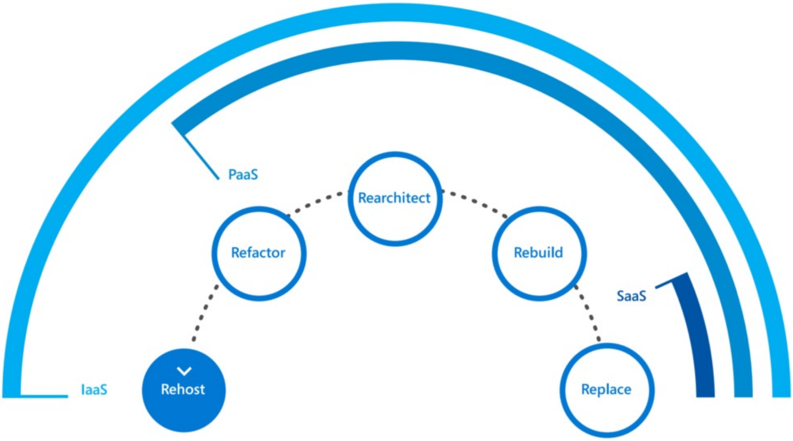
Build new Microsoft Teams Sites for collaboration for internal and external usage. People love Microsoft Teams. You could define 3 team-sets as: Private Team for internal use with only defined memberships. Organization teams for everyone and collaboration teams for customers, internal workers and other peers.

Create a SharePoint Hub for all SharePoint sites – create a frame and design of the requirement and visual for your full organization. From my experience I've seen SharePoint collaboration spaces working where it's simplified and integrated into each team.

Migrate old applications to SharePoint list or PowerApps. I've seen simple apps in Lotus Notes that can easily shift their history to SharePoint lists and PowerApps. PowerBI can help with the transparent reporting and can create a simplified UI for reporting.

4.15 Rethink on-premises

Rehost, Refactor, Rearchitect, rebuild, replace!



Rethink the needs for on-premises.

All collaborations spaces are shifted to Office 365. Your devices are managed with Microsoft 365 Endpoint Manger.

Documents are shifted to OneDrive, Teams and SharePoint.

Authentication and integration with Azure AD is shifted.

Printers with universal Print of different solutions as there are on the market.

Core applications are moved to IaaS and are waiting to become SaaS overtime.

What else is there?

4.16 Build security mechanisms that can be automated

Now, only now, when the shift is completed it is the time to build your security operation.

You could do it upfront but please still have the courage to increase the maturity in general. It's not so helpful to create false positives which don't fix the structural issue(s) or risks that can be prevented easily. If you want to go fast quick wins and quick advises are helping to automate better. Even if it's a shared responsibility.

1. Create a Security Operation and your incident responds can be done within Microsoft Security Center, Azure Sentinel or extended from Microsoft's growing Graph-API. As we are doing now in our Managed Detection and respond 24x7 solution.
2. Build into the next level of modern workplace with Information Protection – which automatic labels classified documents and increases protection of documents. Information Protection can have labels as: Sensitive, internal-only, Public. And are secured. Without authentication they cannot be opened.
3. Get a grip on actionable risks on devices, identities with Microsoft 365 defender in combination with Cloud App Security to identify and isolate risks. Sometimes automatic remediation can be done on simple 'risks' as data exfiltration, mass deletion.

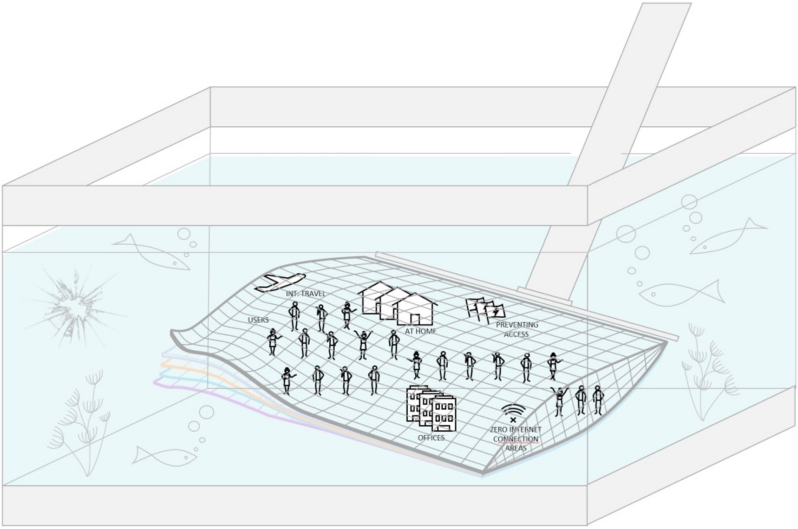
5. Cyber-security in a remote connected world.

5. Cybersecurity in a remote connected world.

5.1 Zero-Trust: The traditional corporate infrastructure is isolated of the outside world

As you can see in this picture by Microsoft in the zero-trust concept organization they did build great solutions in their datacenters on their premises. In their decentralized redundant datacenters with everything in place to have their DR and failover working great.

I'm not blaming smart people which did a great job fixing this massive complex integration to keep everything running 24/7, in their decentral service centers or datacenters.



The solution is... As I've mentioned in my last point. Organizations did a great job, on their premises to get everything working to support their businesses.

Disruption of cloud organizations as Microsoft, Amazon and Google came with scalable and relative quick-deployable solutions. Solutions that didn't require the technical need of the on-premise or 'self-owned' Infrastructure on premises. Microsoft brought a broad spectrum of solutions under: Software-as-a-Service (SaaS), solutions, that are isolated from these corporate environments with plug and play capabilities. SaaS-solutions with quick deployment and management can leverage a lot for these organizations, for these businesses – and this is the most important aspect of it all. **Solutions for organizations, to achieve more**. The support to the ambition of these organizations.

Non-technical driven scenario's, business case and business scenario's.

I think we are (as IT Pro's) sometimes not understanding why disruption came. It is mainly because we were not able to adapt to this scale of changes required to make our organizations more modern. With high-speed implementation.

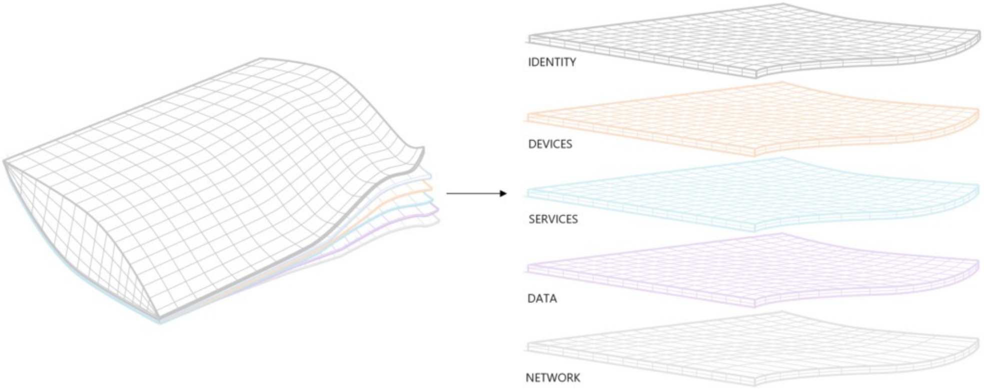
I always give the example when this discussion occurs: Imagine a new Office 365 customer in a cloud scenario. With: Exchange Online, SharePoint Online, Teams Online, Cloud mobile device management. They can start after some hours of implementation.

Imagine the same implementation but then in a private datacenter. How long will it take?

5.2 A new concept of layered approach which kills the fish tank within corporate infrastructure

In the picture below you will see the corporate datacenter with all servers running in virtualized state, segmented with additional security solutions. Segmentation on networking storage and many more services. It's so extreme complex. One mistake could impact everything. next to mistakes: Ransomware, targeted-attacks, phishing attacks, and all other bad-actors took this opportunity to infiltrate and bring this infrastructure down. Sell data.

Bottom-line: it became so complex to react on all aspect of just only the core infrastructure where your servers and services are.



Microsoft didn't invent the layered approach when it comes to: Identity, Devices, Services, Data and Network. It's no new model or real solution set that fixes any problem.

Zero-trust is a way of understanding and integration of your assets to bring them in a layered solution where it cannot touch the asset next to it. Isolation was always the biggest problem of own infrastructure. Even when your organization is huge it's still extremely hard to take everything under control and secured.

5.3 Building your foundation identity management solution

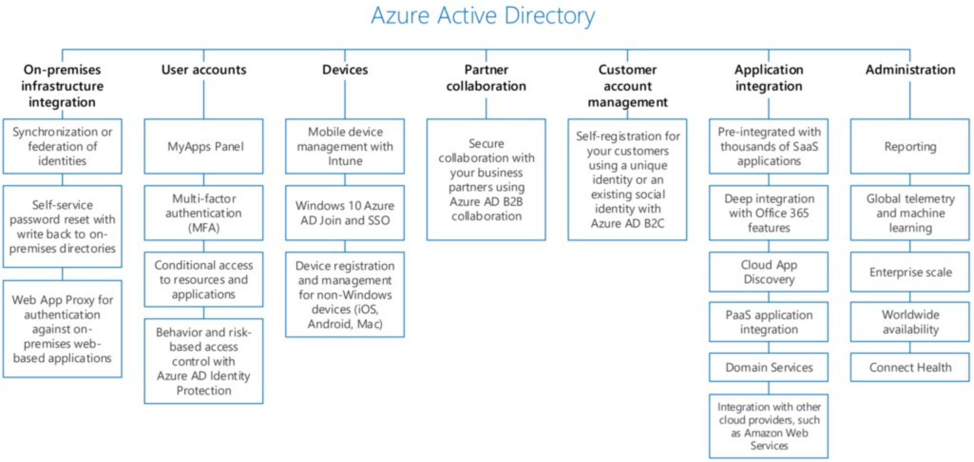
Almost every organization did start with Microsoft Active Directory Servers/services with Windows 2000 or Windows Server 2003. Upgraded to more future-proof versions to integrate better. More features, more integration capabilities, more security. Newer versions.

Cloud solutions were disruptive when Microsoft started with BPOS, before Office 365. Microsoft has built an Identity federation solution based on Microsoft FIM to provision our on-premise active-directory 'accounts' towards Azure Active Directory.

Later the process was well optimized to bring all on-premises identities in sync with Azure AD connect. A modern tool that helps extending your current on-premise Active directory to Azure Active Directory.

But we didn't think Office 365 was the most important part of our core organization.

Azure Active Directory is different than Active Directory On-premise. Is has more features and a more security baselines than Active Directory server. I'm not saying that Azure AD is by design more secure. I'm saying the options are there to start with a better secure baseline. Building blocks. Easier for activations as for example: Azure AD Security Defaults. Maximum value, less complexity faster implementation speed.



Azure Active Directory

- **On-premises infrastructure integration**
  - Synchronization or federation of identities
  - Self-service password reset with write back to on-premises directories
  - Web App Proxy for authentication against on-premises web-based applications
- **User accounts**
  - MyApps Panel
  - Multi-factor authentication (MFA)
  - Conditional access to resources and applications
  - Behavior and risk-based access control with Azure AD Identity Protection
- **Devices**
  - Mobile device management with Intune
  - Windows 10 Azure AD Join and SSO
  - Device registration and management for non-Windows devices (iOS, Android, Mac)
- **Partner collaboration**
  - Secure collaboration with your business partners using Azure AD B2B collaboration
- **Customer account management**
  - Self-registration for your customers using a unique identity or an existing social identity with Azure AD B2C
- **Application integration**
  - Pre-integrated with thousands of SaaS applications
  - Deep integration with Office 365 features
  - Cloud App Discovery
  - PaaS application integration
  - Domain Services
  - Integration with other cloud providers, such as Amazon Web Services
- **Administration**
  - Reporting
  - Global telemetry and machine learning
  - Enterprise scale
  - Worldwide availability
  - Connect Health

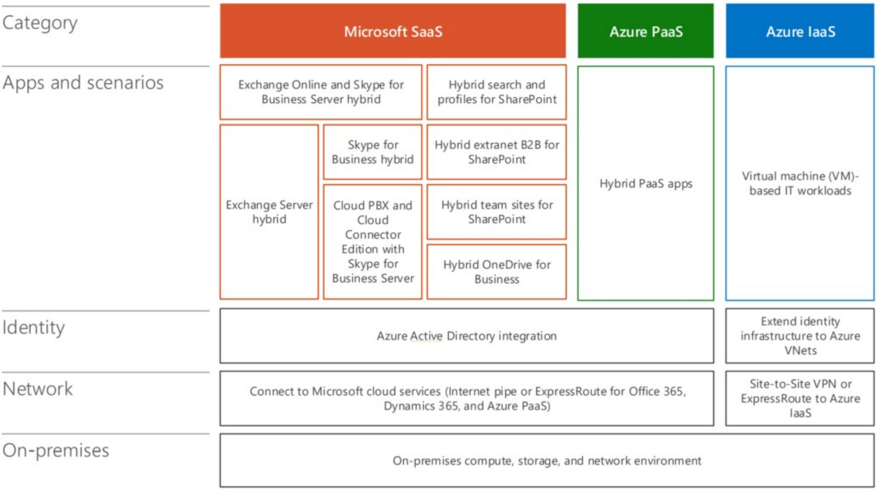
5.4 Enterprise hybrid cloud solution to extend to Office 365 and Azure

Before 2021 a lot of organizations shifted workloads from their on-premises systems infrastructure to Office 365. The most common workload was Exchange

On-premise to Exchange Online. Later these workloads did shift in the Office 365 landscape. For example:

- Fileservers became -> OneDrive, SharePoint or Microsoft Teams
- SharePoint on-premise -> Hybrid -> SharePoint Online
- Mail/Exchange on-premise -> Exchange Online
- Voice/Skype tot hybrid Skype -> Skype Online -> now Microsoft Teams
- with PSTN, Direct routing and all voice capabilities.

As you see I've migrated the biggest workloads on paper and there is nothing left except application servers, other e-mail systems, voice solutions and other solutions. (See Apps & Scenario's)



Category	Microsoft SaaS	Azure PaaS	Azure IaaS
Apps and scenarios	Exchange Online and Skype for Business Server hybrid Hybrid search and profiles for SharePoint Exchange Server hybrid Skype for Business hybrid Cloud PBX and Cloud Connector Edition with Skype for Business Server Hybrid extranet B2B for SharePoint Hybrid team sites for SharePoint Hybrid OneDrive for Business	Hybrid PaaS apps	Virtual machine (VM)-based IT workloads
Identity	Azure Active Directory integration		Extend identity infrastructure to Azure VNets
Network	Connect to Microsoft cloud services (Internet pipe or ExpressRoute for Office 365, Dynamics 365, and Azure PaaS)		Site-to-Site VPN or ExpressRoute to Azure IaaS
On-premises	On-premises compute, storage, and network environment		

As you all know sometimes small infrastructures or some applications are slipping in the architectural designs – I don't think we need to overvalue the fact that in every change some things needs to be taken into account differently.

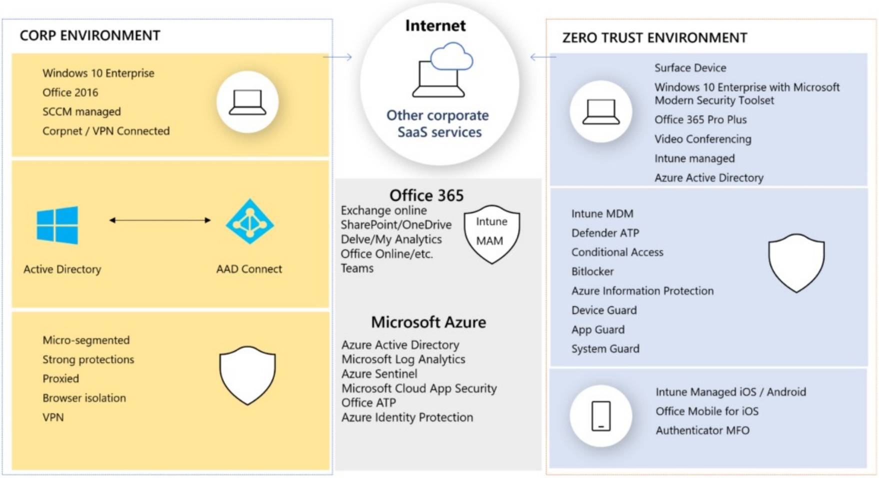
5.5 Endpoint devices and future-proof device management

Devices as Windows XP, Vista, 7, 8, 8,1, Windows 10 (since 2015) 1703, 1706, 1709, 1803, 1806, 1809, 1903, 1909 can be staged by System-Center Configuration Manager in an on-premise solution. And are now brought in a hybrid deployment with Microsoft Endpoint Manager.

Microsoft Endpoint manager is a combination of SCCM + Intune. To get the best of both worlds. Manage workloads from cloud and on-premises.

Example: You could shift the update mechanisms from SCCM towards Endpoint Manager for more cloud control to update at home.

In this overview you see on the right the integration of the current Active-Directory environment towards Azure Active Directory. In the right you see future state building blocks that need to be active on your endpoint devices, to be prepared for the non-phish tank approach. Because most of the time: you already chose Microsoft, Windows 10 and Office 365. The possible scenarios of managing your endpoint devices:



- SCCM only or third-party solutions
- SCCM CO-Management with Endpoint Manager
- Endpoint manager only

How to choose what's right for your organization? What is the right path for modern management? Which products would you need to choose to be ready for a future state workplace?

I'm total fan of going for Endpoint manager in the cloud only world. Because if your new to modern management you have the opportunity to use your hybrid Identity (from on-premises) and your cloud-only joined Azure AD Windows 10 workstation.

Why? Because different than before speed became a huge factor of implementation. And focusing on only the deployment and core Windows 10 enrollment has become less important compared to security implementations and improvements.

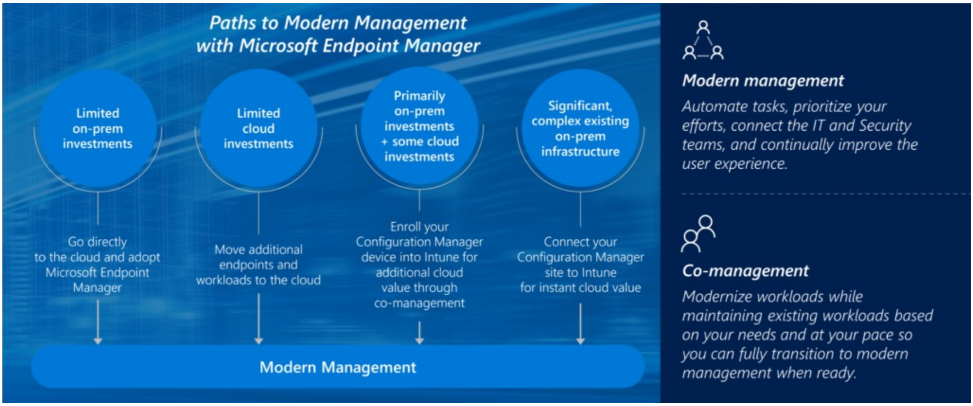
The first reason: The configuration and implementation are easy. Not because I'm lazy to implement more complex solutions but the created simplified standard solutions to manage your Windows 10 Devices are just so important. It's great to have standard sets in Intune that are on or off. It helps the dialogue and the complex discussions and integration in high-speed.

Second reason is: Mobile devices, mobile device management with basis functionality is very easy and transparent with Endpoint Manager. And as we all know: You need to have some scenario's for: BYOD, CYOD, COPE and COBE. BYOD is Bring Your Own Device; CYOD is Choose Your Own Device; COPE is Company Owned/Personally Enabled; and COBO is Company Owned/Business Only. Are you thinking this is the bla bla cool term discussion? Let's get that sorted out: Are you able to securely work on your mobile applications and protect your companies IP. Do you know where your company data is located?

Third Reason: The security maturity and implementation effort has pro's: Bitlocker activation, Windows Hello For Business working great, running Cloud-only, easy activation. I believe segmentation of this device layer is important to not have lateral movement with domain joined devices connected on-premises. It's not even technical possible if the device is not trusted. (zero-trust)

Fourth reason: No hybrid complexity, easier staging with Windows Autopilot. Staging from anywhere. Not possible in hybrid scenario's, at the moment. It's announced it will be possible soon.

Fifth reason: Go Cloud. If you have no on-premises infrastructure left and are able to go without ‘traditional’ domain controllers to Azure AD or ADDS. The baseline is the most important real tangible factor. There are more capabilities easier to implement. Long-term is the real reason.



Paths to Modern Management with Microsoft Endpoint Manager

Limited on-prem investments — Go directly to the cloud and adopt Microsoft Endpoint Manager

Limited cloud investments — Move additional endpoints and workloads to the cloud

Primarily on-prem investments + some cloud investments — Enroll your Configuration Manager device into Intune for additional cloud value through co-management

Significant, complex existing on-prem infrastructure — Connect your Configuration Manager site to Intune for instant cloud value

Modern Management

Modern management

Automate tasks, prioritize your efforts, connect the IT and Security teams, and continually improve the user experience.

Co-management

Modernize workloads while maintaining existing workloads based on your needs and at your pace so you can fully transition to modern management when ready.

Why should you choose for CO-Management and what are decision points?

When you are not in a hurry moving to full-cloud. And for example it is defined you will shift in 2025. And still will keep your on-premises core-environment intact until then.

When you have big task-sequence and big deployment of software that is not possible to bring to Endpoint Manager. But more important is strategy. It will be strange if you keep SCCM without any other workload on-premise. Choose strategic, long term.

If strategy of full-cloud is defined. Don't invest in co-management. For example: No business-critical application service is running on-premises, shift to EndPoint Manager. It's better to make the investment in modern tools compared to well know configuration manager.

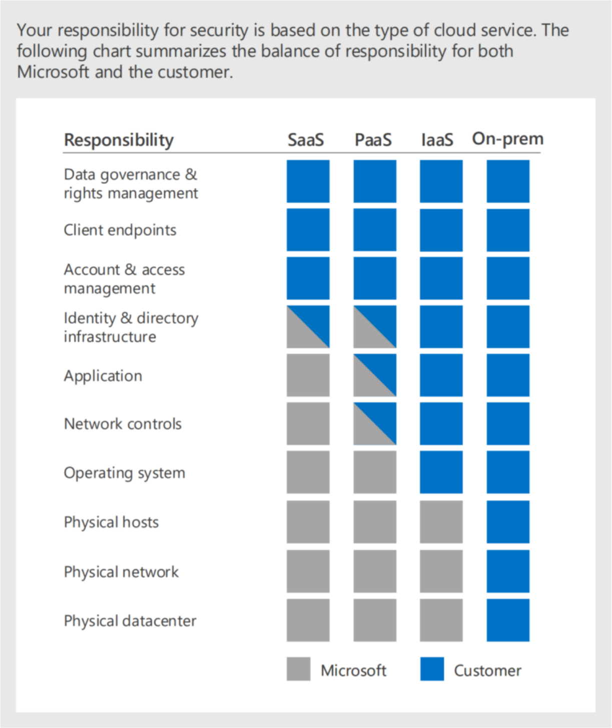
When you have 20 language packs and custom scripts. Sometimes hard decisions need to be made to be more flexible in a later stadium. Again, Strategic decision.

5.6 Services, servers and infrastructure

It's all about responsibility, complexity, standards, governance, way of stabilizing your businesses critical systems.

Responsibility and Security: As you can see in this matrix thanks to the shift of On-premise servers, appliances, services running Windows Server or different operations systems the ownership is in the organizations hands.

The downside in general is security. It's difficult to segment, patch, upgrade, update and keep track of risks in the attack chain. Servers are integrated with active directory. Next to Security TCO is important. Did you know that we spend a lot of our time doing core-infrastructure tasks to keep everything running? It is very critical infrastructure. Do we really want to keep on working on and supporting this infrastructure when there are other options? It's an illusion to think organizations can keep up evolving and transforming when the focus is not shifted and the battle of cloud focus is not yet won.

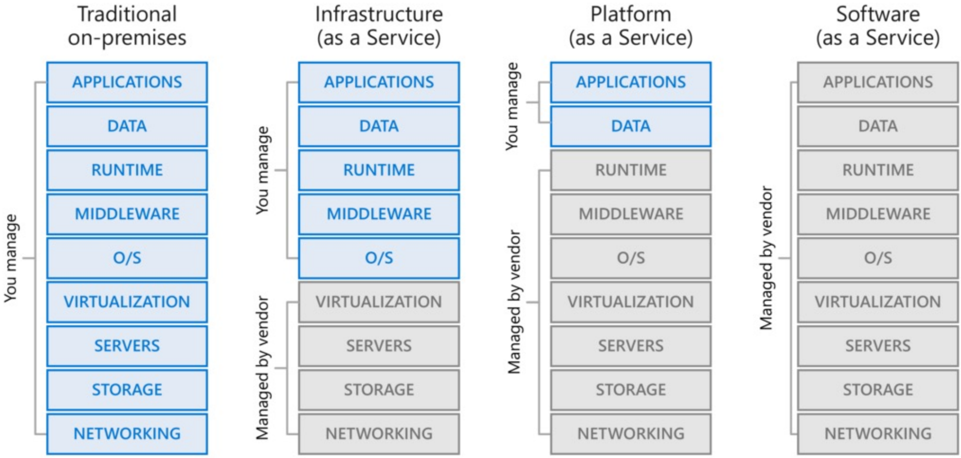


Your responsibility for security is based on the type of cloud service. The following chart summarizes the balance of responsibility for both Microsoft and the customer.

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	🟦	🟦	🟦	🟦
Client endpoints	🟦	🟦	🟦	🟦
Account & access management	🟦	🟦	🟦	🟦
Identity & directory infrastructure	◪	◪	🟦	🟦
Application	⬜	◪	🟦	🟦
Network controls	⬜	◪	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

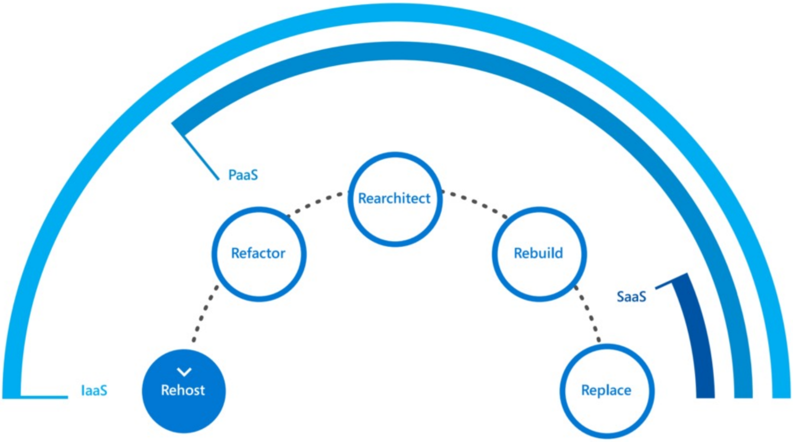
⬜ Microsoft 🟦 Customer

The next diagram shows the responsibilities within Cloud services – important here is having to leave some things behind that are commodity and create opportunity for infrastructure- and software engineers and architects to build on the core-solutions and not on the datacenters in general.



“Rehost, Refractor, Rearchitect, rebuild, replace” – IF you want to shift to a modern approach redesigning to Software as a service, when possible, is very important.

Example: Azure File Server, Azure SQL. No Windows server 2016 running SQL instance(s). Just a SaaS solution. Easier for technical workers.



5.7 Data (Documents)

Data maturity. Automatic processing. Automation, you get the point. (document)data is crucial and needs protection. Document data is the core of every organization. And still we are sending documents over e-mail, sharing over third-party solutions that are not trusted etc.

The Information lifecycle is starting when the document creation is taking place. From the start 'document controls' are not included so the opportunity to spread documents is massive.

We need a consolidated approach to fix the document data 'problem' and discovery of security risks, compliance. **We need to take back control of corporate data**. It's sometimes difficult to understand that companies are building data warehouses with high-end security and leave the door open when it comes to information/ documents management. We are building super complex systems with machine learning, intelligent architectures for modern needs. With super smart people – but we leave the "core workplace behind".

Trust / Platform / Decide -> Choose Microsoft. If you chose Office 365 to collaborate better and you don't trust the environment, you made the wrong choice. I mean, use the technology to make your environment more secure. Don't use it if it's just for mail. The technology goes beyond the tool itself.

Migrate personal documents to OneDrive, Organizational document to SharePoint or Teams and other application data to Azure Fileserver or different solutions.

The main reason is data control. When fileservers and local copies are gone Microsoft 365 cloud can deliver automated labeling and classification or at least insights on confidential data. We lack data-control. Not even the 'understanding' of document movement in our organizations.

Cloud App Security. Cloud App Security can help you remediate and take actions, when necessary, discover document flows and help to set rules on documents when the risk of data-leakage is there. Information lifecycle can be done by Cloud App Security to fix the 'complex' solutions when we made them complex. There is nothing easier to manage than Office 365: Teams, SharePoint, Yammer, Exchange when this is the only platform used.

Security and governance in Microsoft 365 are hard. But it's even harder if you also have on-premises resources and non-controlled instances. The pros of only O365 are you can deliver actionable insights.

5.8 Network

Collaboration-based traffic in Cloud App Security can help to understand risks such as data-exfiltration towards the internet or a different network location. When combining the log data of network devices with Microsoft 365 the opportunity is there to also capture the full environment.

Every organization needs a stable network, shaping, priorities and all other things to regulate network infrastructure. It is super important. Still, it’s best to stop trusting (Zero-Trust) our own networks as much as we did, before. Because the silo walls are gone. The crucial organization data shifted to somewhere else. In the public, private or non-local Cloud.

6. Automation and intelligent Security.

6. Automation and intelligent Security.

6.1 The basics need to be implemented, first

I've written some basic best practices for a safer workplace below. I think that sometimes we dare to think that 'intelligent Security' is fixing the basics. Sorry it's not. When doing automation, the maturity should be there to have **standard sets**, policies defined.

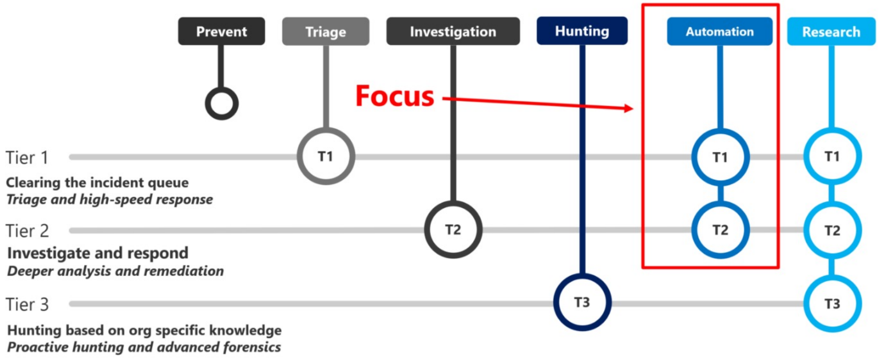
- Multi-Factor Authentication or Azure Security Defaults.
- Conditional Access for trusted parameters – easier login's – and more security.
- Connect your devices to Azure AD with Endpoint Manager to 'block' unwanted devices.
- Risky User Sign-in policies. Good definitions of security policies.
- Self-Service Password Reset to help everyone to reset their own password.
- Create control on lifecycle management of identities. Expiration, onboarding, offboarding etc.

6.2 Microsoft is delivering automated Security Operations (SecOps) for any organization

Microsoft is delivering automated response if you have a security aware and mature organization. In the ideal world, I know. But we need to make the world more aware of the risks and the impact of a security-breach.

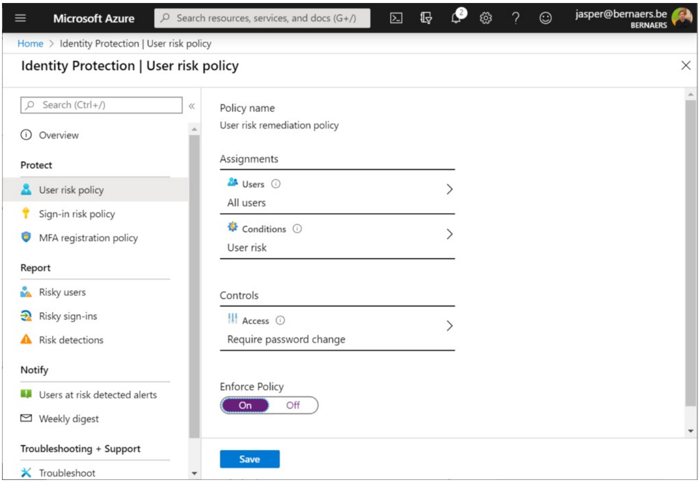
If you have created automated tasks in your organization, you could tackle a lot of all the alerts.

- **Tier 1**: Clearing the incident queue – Triage and high-speed response
- **Tier 2**: Investigate and respond – Deeper analysis and remediation
- **Tier 3**: Hunting based on org specific knowledge – Proactive hunting and advanced forensics


Prevent
Triage
Investigation
Hunting
Automation
Research
Focus
Tier 1
Clearing the incident queue
Triage and high-speed response
Tier 2
Investigate and respond
Deeper analysis and remediation
Tier 3
Hunting based on org specific knowledge
Proactive hunting and advanced forensics
T1
T2
T3

Practical examples of T1 and T2 response and remediate

Example 1. Identity protection: Require Password Change when the risk is high. Create a process that describes the action required as: Call user – validate risk – validate credentials (real person).



Identity Protection | User risk policy

Policy name
User risk remediation policy

Assignments

Users
All users

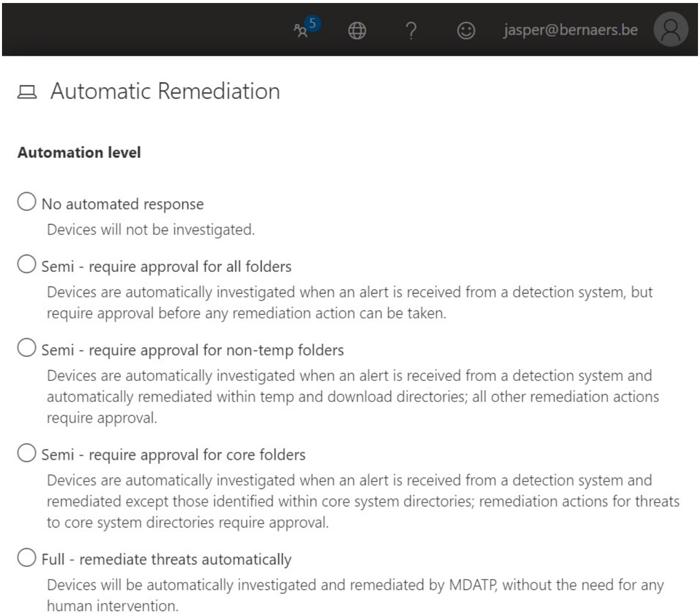
Conditions
User risk

Controls

Access
Require password change

Enforce Policy
On Off

Example 2. Automatic Remediation when suspicious events are happening. If you don't want to do anything set remediation to automatically and build a partnership with Microsoft Engineers to consult when threats are around the corner. This is a holistic position. You need Security specialists to start from scratch.



Automatic Remediation

Automation level

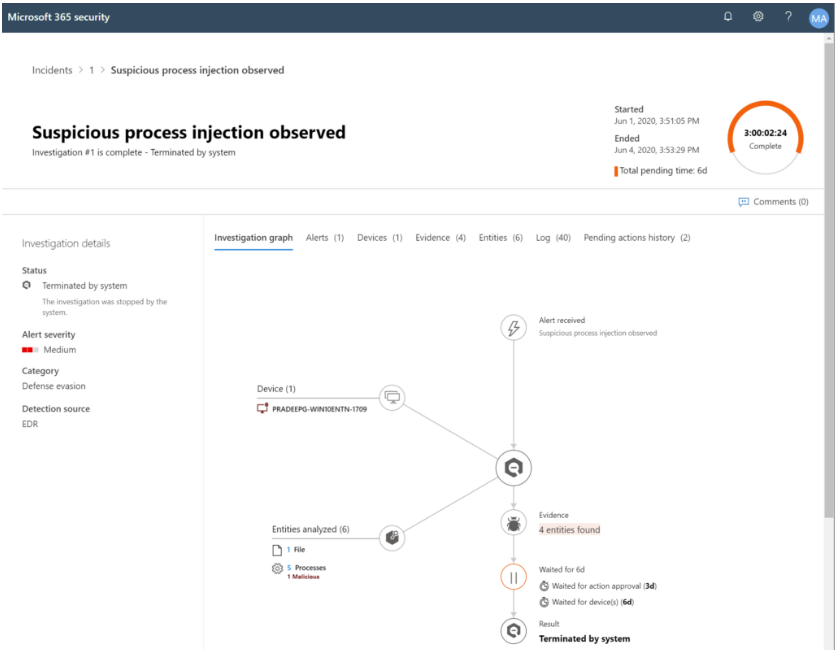
○ No automated response
Devices will not be investigated.

○ Semi - require approval for all folders
Devices are automatically investigated when an alert is received from a detection system, but require approval before any remediation action can be taken.

○ Semi - require approval for non-temp folders
Devices are automatically investigated when an alert is received from a detection system and automatically remediated within temp and download directories; all other remediation actions require approval.

○ Semi - require approval for core folders
Devices are automatically investigated when an alert is received from a detection system and remediated except those identified within core system directories; remediation actions for threats to core system directories require approval.

○ Full - remediate threats automatically
Devices will be automatically investigated and remediated by MDATP, without the need for any human intervention.



Microsoft 365 security

Incidents > 1 > Suspicious process injection observed

Suspicious process injection observed

Investigation #1 is complete - Terminated by system

Started
Jun 1, 2020, 3:51:05 PM
Ended
Jun 4, 2020, 3:53:29 PM
Total pending time: 6d

3:00:02:24
Complete

Comments (0)

Investigation details

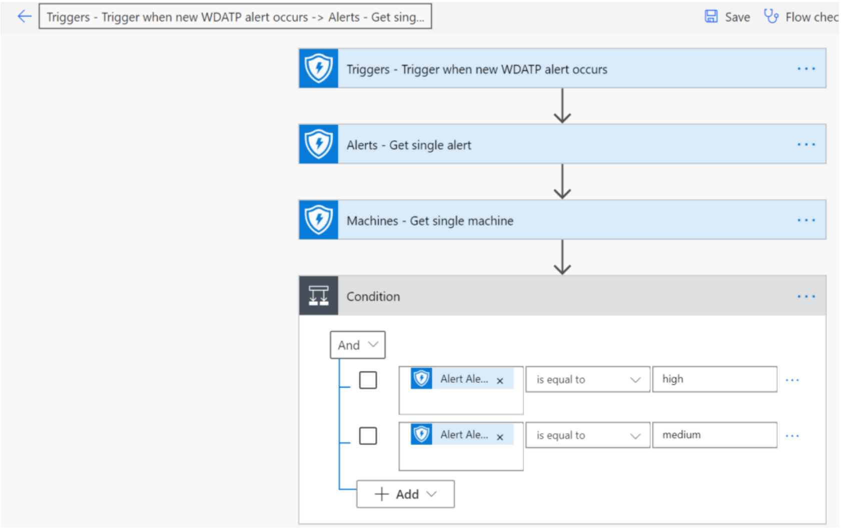
Status
Terminated by system
The investigation was stopped by the system.

Alert severity
Medium

Category
Defense evasion

Detection source
EDR

Example 3. Isolate a machine when risk is detected. You can use Microsoft Power Automate to do automated response when events occur. The possibilities built-in without any code and development are huge.



Triggers - Trigger when new WDATP alert occurs -> Alerts - Get sing...

Triggers - Trigger when new WDATP alert occurs

Alerts - Get single alert

Machines - Get single machine

Condition

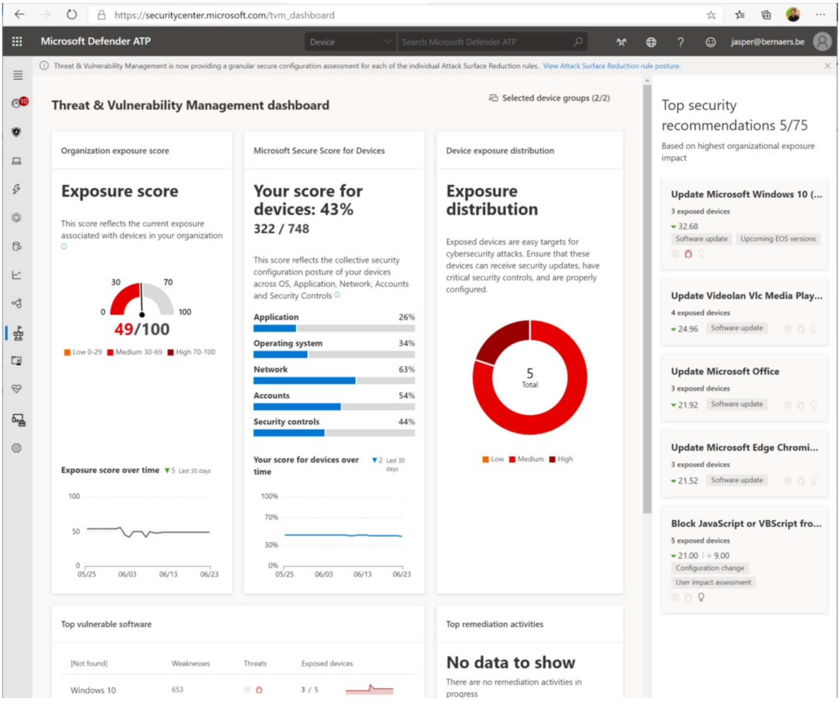
And

□ Alert Ale... × | is equal to | high

□ Alert Ale... × | is equal to | medium

Identify(1) and Protect(2)

What you could do to Identify and protect your organization is work with the: Threat & Vulnerability Management dashboard to map actions on your road-map to implement. 5 top Security recommendations are brought by Microsoft, as example.



https://securitycenter.microsoft.com/tvm_dashboard

Microsoft Defender ATP

Device | Search Microsoft Defender ATP | jasper@bernaers.be

Threat & Vulnerability Management is now providing a granular secure configuration assessment for each of the individual Attack Surface Reduction rules. View Attack Surface Reduction rule posture.

Threat & Vulnerability Management dashboard

Selected device groups (2/2)

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization

49/100

🟧 Low 0-29 🟥 Medium 30-69 🟥 High 70-100

Exposure score over time ▼5 Last 30 days

Microsoft Secure Score for Devices

Your score for devices: 43%

322 / 748

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls

Application	26%
Operating system	34%
Network	63%
Accounts	54%
Security controls	44%

Your score for devices over time ▼2 Last 30 days

Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.

🟧 Low 🟥 Medium 🟥 High

Top security recommendations 5/75

Based on highest organizational exposure impact

Update Microsoft Windows 10 (...
3 exposed devices
▼32.68
Software update | Upcoming EOS versions

Update Videolan Vlc Media Play...
4 exposed devices
▼24.96 Software update

Update Microsoft Office
3 exposed devices
▼21.92 Software update

Update Microsoft Edge Chromi...
3 exposed devices
▼21.52 Software update

Block JavaScript or VBScript fro...
5 exposed devices
▼21.00 | + 9.00
Configuration change
User impact assessment

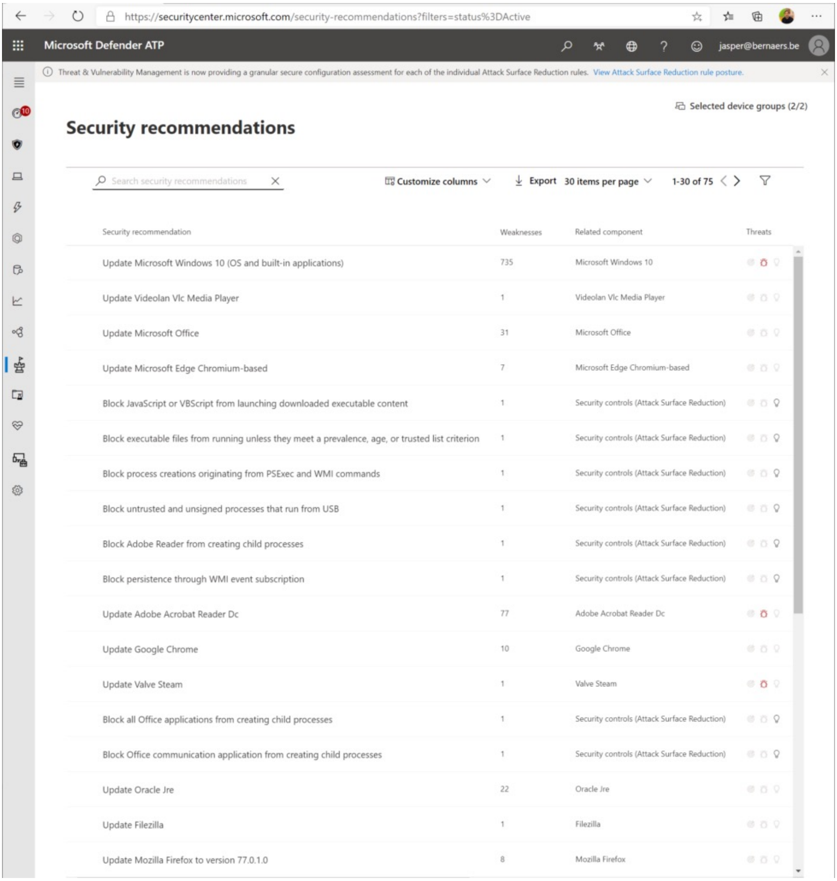
Top vulnerable software

[Not found]	Weaknesses	Threats	Exposed devices
Windows 10	653		3 / 5

Top remediation activities

No data to show

There are no remediation activities in progress



https://securitycenter.microsoft.com/security-recommendations?filters=status%3DActive

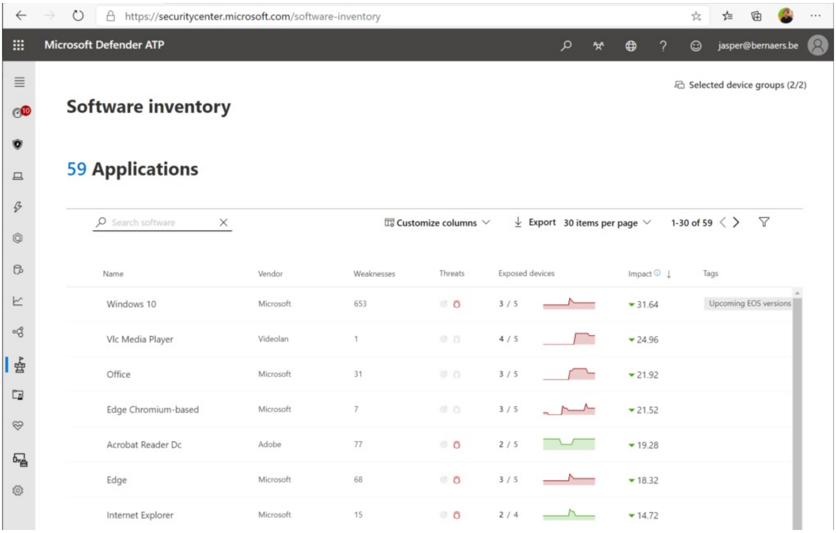
Threat & Vulnerability Management is now providing a granular secure configuration assessment for each of the individual Attack Surface Reduction rules. View Attack Surface Reduction rule posture.

Selected device groups (2/2)

Security recommendations

Security recommendation	Weaknesses	Related component	Threats
Update Microsoft Windows 10 (OS and built-in applications)	735	Microsoft Windows 10	
Update Videolan Vlc Media Player	1	Videolan Vlc Media Player	
Update Microsoft Office	31	Microsoft Office	
Update Microsoft Edge Chromium-based	7	Microsoft Edge Chromium-based	
Block JavaScript or VBScript from launching downloaded executable content	1	Security controls (Attack Surface Reduction)	
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	1	Security controls (Attack Surface Reduction)	
Block process creations originating from PSExec and WMI commands	1	Security controls (Attack Surface Reduction)	
Block untrusted and unsigned processes that run from USB	1	Security controls (Attack Surface Reduction)	
Block Adobe Reader from creating child processes	1	Security controls (Attack Surface Reduction)	
Block persistence through WMI event subscription	1	Security controls (Attack Surface Reduction)	
Update Adobe Acrobat Reader Dc	77	Adobe Acrobat Reader Dc	
Update Google Chrome	10	Google Chrome	
Update Valve Steam	1	Valve Steam	
Block all Office applications from creating child processes	1	Security controls (Attack Surface Reduction)	
Block Office communication application from creating child processes	1	Security controls (Attack Surface Reduction)	
Update Oracle Jre	22	Oracle Jre	
Update Filezilla	1	Filezilla	
Update Mozilla Firefox to version 77.0.1.0	8	Mozilla Firefox	

Security Recommendations:
Find the critical gaps. Put them towards the operational team. A process needs to be defined.



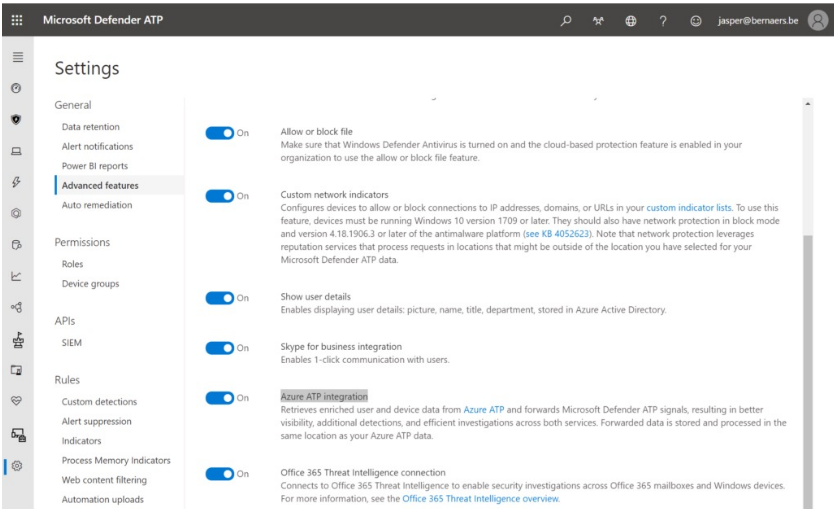
https://securitycenter.microsoft.com/software-inventory

Software inventory

59 Applications

Name	Vendor	Weaknesses	Threats	Exposed devices	Impact	Tags
Windows 10	Microsoft	653		3 / 5	31.64	Upcoming EOS versions
Vlc Media Player	Videolan	1		4 / 5	24.96	
Office	Microsoft	31		3 / 5	21.92	
Edge Chromium-based	Microsoft	7		3 / 5	21.52	
Acrobat Reader Dc	Adobe	77		2 / 5	19.28	
Edge	Microsoft	68		3 / 5	18.32	
Internet Explorer	Microsoft	15		2 / 4	14.72	

Software inventory:
Easiness of understanding the temperature and the required actions to make these risks go away. Again process.



Settings

On — Allow or block file
Make sure that Windows Defender Antivirus is turned on and the cloud-based protection feature is enabled in your organization to use the allow or block file feature.

On — Custom network indicators
Configures devices to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists. To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform (see KB 4052623). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender ATP data.

On — Show user details
Enables displaying user details: picture, name, title, department, stored in Azure Active Directory.

On — Skype for business integration
Enables 1-click communication with users.

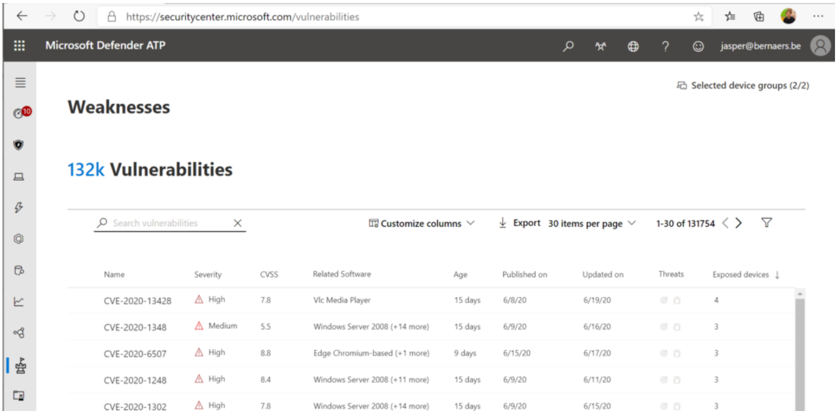
On — Azure ATP integration
Retrieves enriched user and device data from Azure ATP and forwards Microsoft Defender ATP signals, resulting in better visibility, additional detections, and efficient investigations across both services. Forwarded data is stored and processed in the same location as your Azure ATP data.

On — Office 365 Threat Intelligence connection
Connects to Office 365 Threat Intelligence to enable security investigations across Office 365 mailboxes and Windows devices. For more information, see the Office 365 Threat Intelligence overview.

Integrate ATP for on-premises alerts from lateral movements, plain text passwords, pass-the-ticket/hash to understand which alerts occur.

Detect (3)

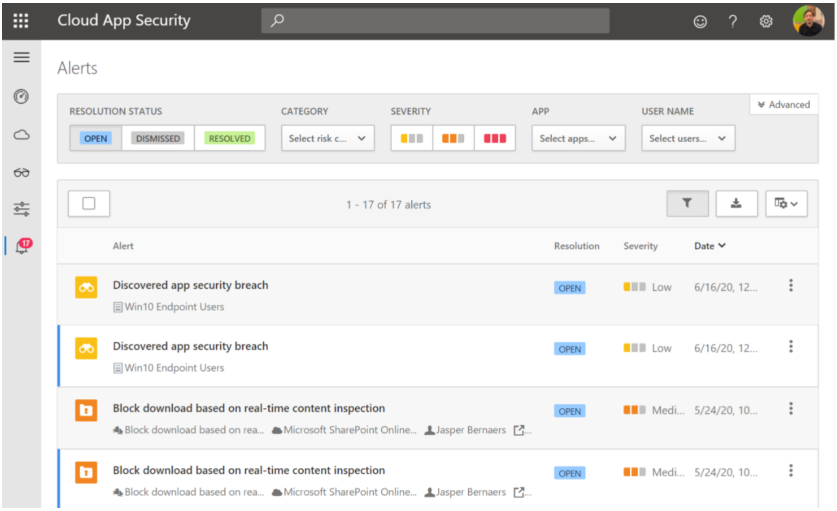
Weaknesses in Security Center: Easy to bring these in the first process and create processes with service levels to fix these gaps.



Weaknesses

132k Vulnerabilities

Name	Severity	CVSS	Related Software	Age	Published on	Updated on	Threats	Exposed devices ↓
CVE-2020-13428	High	7.8	Vlc Media Player	15 days	6/8/20	6/19/20		4
CVE-2020-1348	Medium	5.5	Windows Server 2008 (+14 more)	15 days	6/9/20	6/16/20		3
CVE-2020-6507	High	8.8	Edge Chromium-based (+1 more)	9 days	6/15/20	6/17/20		3
CVE-2020-1248	High	8.4	Windows Server 2008 (+11 more)	15 days	6/9/20	6/11/20		3
CVE-2020-1302	High	7.8	Windows Server 2008 (+14 more)	15 days	6/9/20	6/15/20		3

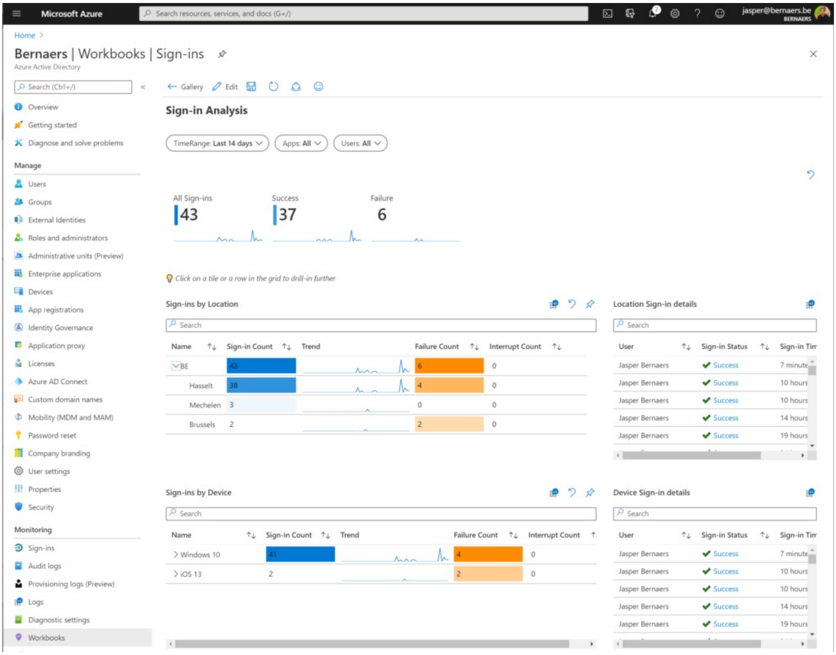


Alerts

1 - 17 of 17 alerts

Alert	Resolution	Severity	Date
Discovered app security breach Win10 Endpoint Users	OPEN	Low	6/16/20, 12...
Discovered app security breach Win10 Endpoint Users	OPEN	Low	6/16/20, 12...
Block download based on real-time content inspection Block download based on rea... Microsoft SharePoint Online... Jasper Bernaers	OPEN	Medi...	5/24/20, 10...
Block download based on real-time content inspection Block download based on rea... Microsoft SharePoint Online... Jasper Bernaers	OPEN	Medi...	5/24/20, 10...

Cloud App Security:
Find anomalies based on Alerts of sign in or device based.



Bernaers | Workbooks | Sign-ins
Azure Active Directory

Sign-in Analysis

TimeRange: **Last 14 days** | Apps: **All** | Users: **All**

All Sign-ins 43 | Success 37 | Failure 6

Click on a tile or a row in the grid to drill-in further

Sign-ins by Location

Name	Sign-in Count	Trend	Failure Count	Interrupt Count
BE	43		6	0
Hasselt	38		4	0
Mechelen	3		0	0
Brussels	2		2	0

Location Sign-in details

User	Sign-in Status	Sign-in Tir
Jasper Bernaers	✓ Success	7 minute
Jasper Bernaers	✓ Success	10 hours
Jasper Bernaers	✓ Success	10 hours
Jasper Bernaers	✓ Success	14 hours
Jasper Bernaers	✓ Success	19 hours

Sign-ins by Device

Name	Sign-in Count	Trend	Failure Count	Interrupt Count
Windows 10	41		4	0
iOS 13	2		2	0

Device Sign-in details

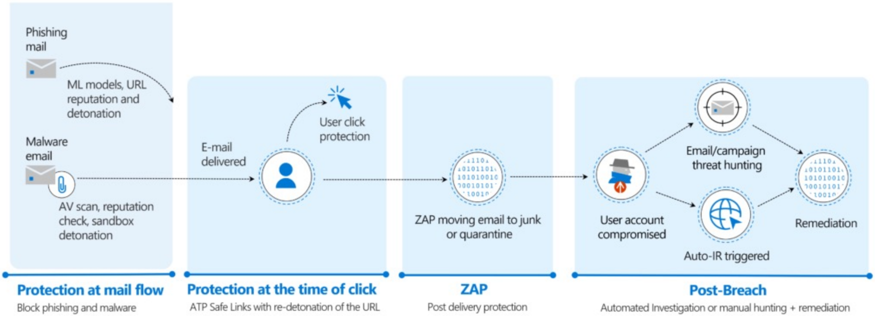
User	Sign-in Status	Sign-in Tir
Jasper Bernaers	✓ Success	7 minute
Jasper Bernaers	✓ Success	10 hours
Jasper Bernaers	✓ Success	10 hours
Jasper Bernaers	✓ Success	14 hours
Jasper Bernaers	✓ Success	19 hours

Azure Workbooks for sign-in analyses

Other possibilities: Risky Sign-ins, Security center, Log Analytics queries,..

Respond (4)

Responding is actually doing something to prevent that the breached device or identity is being taking care of. It's doing an action to prevent different users from


Phishing mail
ML models, URL reputation and detonation
Malware email
AV scan, reputation check, sandbox detonation
E-mail delivered
User click protection
ZAP moving email to junk or quarantine
User account compromised
Email/campaign threat hunting
Auto-IR triggered
Remediation
Protection at mail flow
Block phishing and malware
Protection at the time of click
ATP Safe Links with re-detonation of the URL
ZAP
Post delivery protection
Post-Breach
Automated Investigation or manual hunting + remediation

having the same risk. As for example isolate a device when doing research. Or locking an account if the risks is valid. Also work with ATP.

Automatic investigation can start with: User-reporting a phishing email or a user clicks a malicious link.

Recover (5)

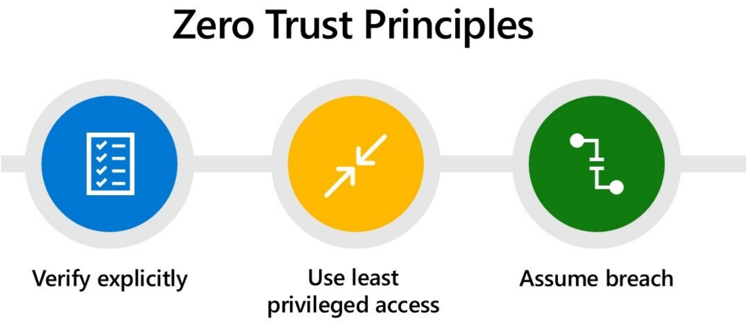
Ransomware detection and recovering your files in OneDrive. (built-in)
SharePoint Site-restore for collections and sites. (built-in)
Backup with Microsoft technology of third-party.
Azure Restore/Back-up, SQL Service backup/...
In general disaster recovery plan

6.3 Intelligent Security

“The evidence is clear—the old security paradigm of building an impenetrable fortress around your resources and data is simply not viable against today’s challenges. Remote and hybrid work realities mean people move fluidly between work and personal lives, across multiple devices, and with increased collaboration both inside and outside of organizational boundaries. Entry points for attacks—identities, devices, apps, networks, infrastructure, and data—live outside the protections of traditional perimeters. The modern digital estate is distributed, diverse, and complex." -> This new reality requires a Zero Trust approach.

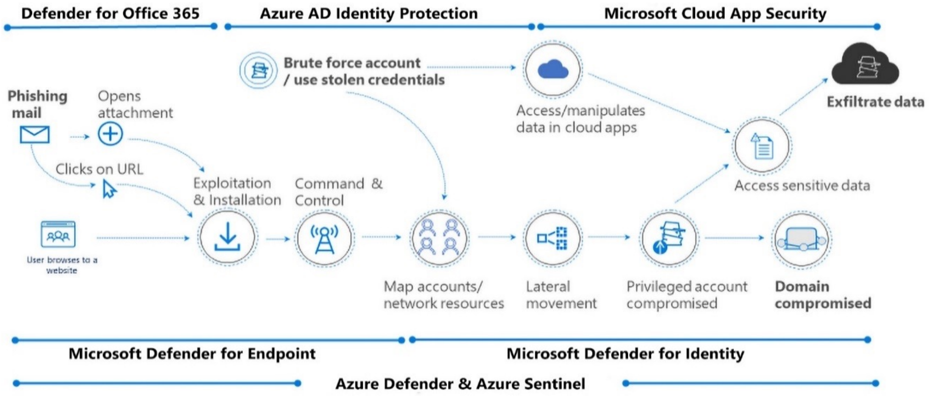
Impact of Zero Trust

- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- Access to trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task.
- Assets should always act as if an attacker is present on the enterprise network.



7.
The Value of Microsoft 365 E5.

7. The Value of Microsoft 365 E5.


Defender for Office 365
Azure AD Identity Protection
Microsoft Cloud App Security
Brute force account / use stolen credentials
Phishing mail
Opens attachment
Clicks on URL
User browses to a website
Exploitation & Installation
Command & Control
Access/manipulates data in cloud apps
Exfiltrate data
Access sensitive data
Map accounts/ network resources
Lateral movement
Privileged account compromised
Domain compromised
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Azure Defender & Azure Sentinel

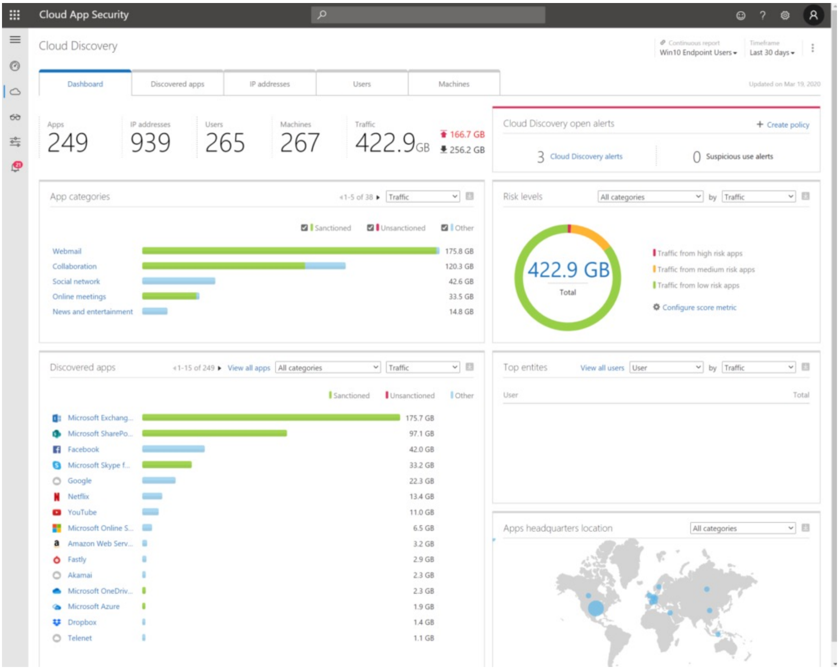
7.1 Protection across the attack kill chain

This picture shows the value of Microsoft 365 E5. A lot of interactions today in conversations are landing in product compare between antivirus solution or segmented parts of Microsoft 365 E5. The questions here are: Are you going to deep-dive in the license compare strategy of your current antivirus? Do you have a separated anti-spam solution, Azure AD Protection, Cloud App Security, or more important: Can you handle a chain that can be automated to prevent security incidents?

7.2 Cloud App Security

Cloud App Security shows you exactly whether data is passing on all endpoints. Document data, lateral movements, usage of applications, global traffic, count of applications in use in your organization. Cloud App Security can also understand your sessions as broker and can stop untrusted connections.

Thanks to the native integration in Microsoft Defender for Endpoint and Edge-based web security technology integration. Risk levels, GDPR 'proof' Cloud applications, also devices, users and IP addresses can be investigated to understand and control.

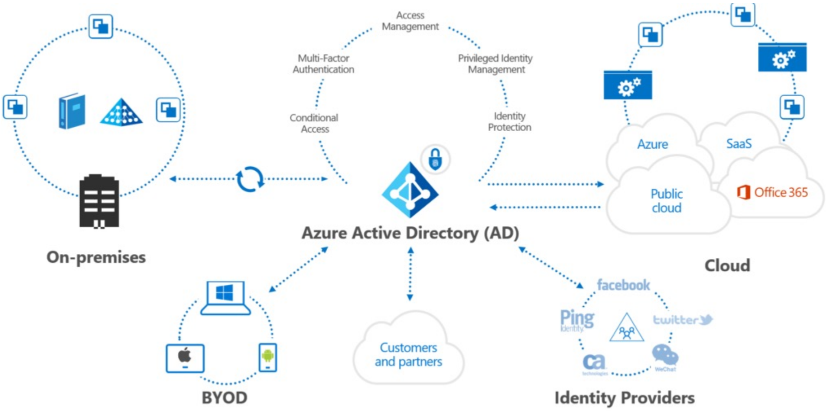


You are capable to bring network device logging in CASB to have more insights. This feature is out-of-the box available and just needs activation and parametrization.

For this technology Cloud applications are a driver for usage to have more insights and controls.

7.3 Identity & Access management

Because of simplified Identity management organizations are able to work with Security perimeters to protect their users and organization. Because of this simplified configuration and implementation users will be able to reset their own password, control their own devices, or configure additional security components.



7.4 Self-Service Password Reset (SSPR)

The SSPR possibility is an Azure Active Directory (AD) feature that enables users to reset their passwords without contacting IT staff for help. People can unblock themselves and continue working no matter where they are. Ideal solution for more self-driven organization.

7.5 Managed Mobile Device

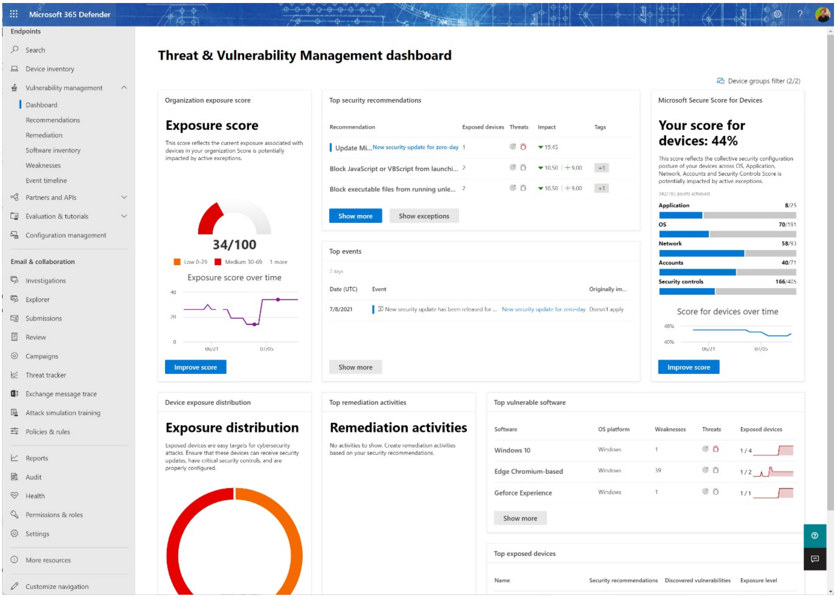
"Cloud intelligence drives management". Use Autopilot to roll-out new devices and increase productivity, reduce help-desk costs and provide the best employee experience. Manage you Windows 10 or 11 devices and your mobile devices.

Tip: Stop allowing personal devices without taking control of organization data. Use mobile application management (MAM) but be diplomatic for end-users. I would go for the pin code at least.

7.6 Microsoft Defender Security Center Security operations dashboard

The Security operations dashboard is where the endpoint detection and response capabilities are coming together. The Microsoft Security Center operation dashboard provides a high-level overview of where detections were seen and highlights where response actions are needed.

The portal integrated multiple facets of the workplace into one place and creates useful insights to bring your workplace to a higher security level.



Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization Score is potentially impacted by active exceptions.

Top security recommendations

Recommendation	Exposed devices	Threats	Impact	Tags
Update Mi... New security update for zero-day	1		▼19.45	
Block JavaScript or VBScript from launchi...	2		▼10.50 | +9.00	+1
Block executable files from running unle...	2		▼10.50 | +9.00	+1

Top events

7 days

Date (UTC)	Event	Originally im...
7/8/2021	New security update has been released for ... New security update for zero-day	Doesn't apply

Microsoft Secure Score for Devices

Your score for devices: 44%

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score is potentially impacted by active exceptions.

342/785 points achieved

Application	8/25
OS	70/191
Network	58/93
Accounts	40/71
Security controls	166/405

Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.

Top remediation activities

Remediation activities

No activities to show. Create remediation activities based on your security recommendations.

Top vulnerable software

Software	OS platform	Weaknesses	Threats	Exposed devices
Windows 10	Windows	1		1 / 4
Edge Chromium-based	Windows	39		1 / 2
Geforce Experience	Windows	1		1 / 1

Top exposed devices

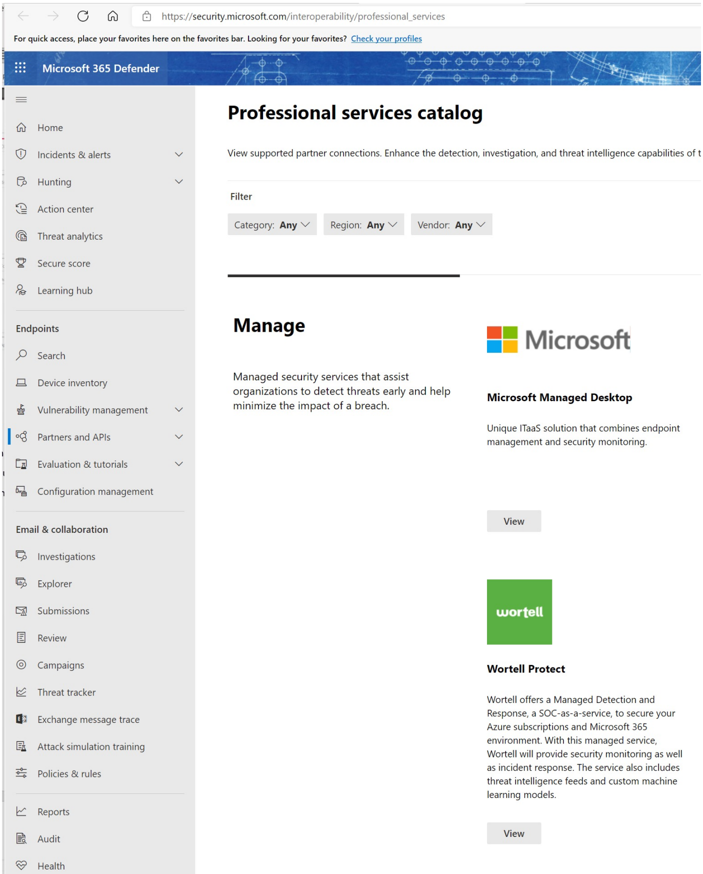
Name	Security recommendations	Discovered vulnerabilities	Exposure level

Example: Threat & Vulnerability Management dashboard

You can also find us in the professional services catalog to work on: Managed security services that assist organizations to detect threats early and help minimize the impact of a breach.

7.7 Identity driven Security

Because of the use of a single identity in Azure. Or hybrid synced from your local Active Directory, services organizations will be able to protect and automatically act when necessary and request for an update of your password if breached. Ask MFA when your device is not trusted. etc.. let your users update their password from home. Increase productivity.



Professional services catalog

View supported partner connections. Enhance the detection, investigation, and threat intelligence capabilities of t

Filter

Manage

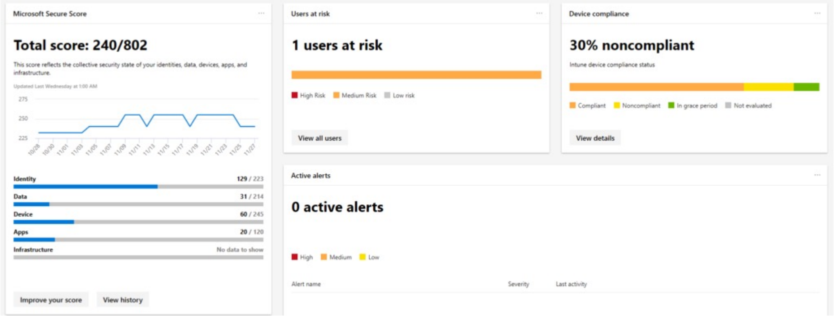
Managed security services that assist organizations to detect threats early and help minimize the impact of a breach.

Microsoft Managed Desktop

Unique ITaaS solution that combines endpoint management and security monitoring.

Wortell Protect

Wortell offers a Managed Detection and Response, a SOC-as-a-service, to secure your Azure subscriptions and Microsoft 365 environment. With this managed service, Wortell will provide security monitoring as well as incident response. The service also includes threat intelligence feeds and custom machine learning models.



Microsoft Secure Score

Total score: 240/802

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

Updated Last Wednesday at 1:00 AM

Identity	129 / 223
Data	31 / 214
Device	60 / 245
Apps	20 / 120
Infrastructure	No data to show

Users at risk

1 users at risk

Device compliance

30% noncompliant

Intune device compliance status

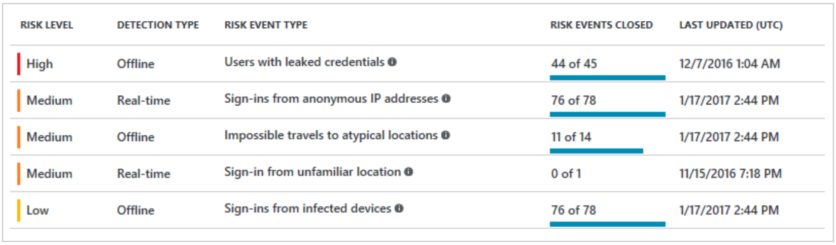
Active alerts

0 active alerts

Alert name	Severity	Last activity

7.8 Risky Sign-ins

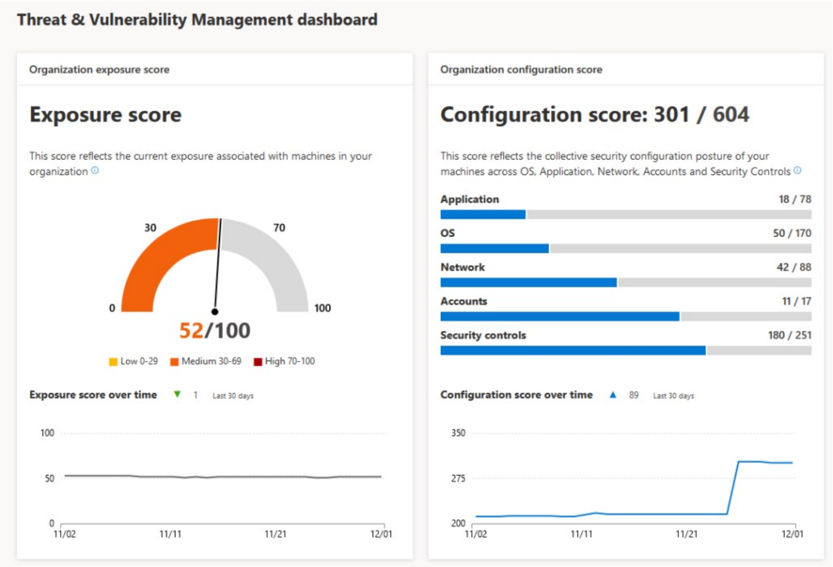
This great feature will bring based on cloud intelligence insights to understand the RISK of a user. For example unfamiliar location, anonymous IP addresses, leaked credentials..



RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials	44 of 45	12/7/2016 1:04 AM
Medium	Real-time	Sign-ins from anonymous IP addresses	76 of 78	1/17/2017 2:44 PM
Medium	Offline	Impossible travels to atypical locations	11 of 14	1/17/2017 2:44 PM
Medium	Real-time	Sign-in from unfamiliar location	0 of 1	11/15/2016 7:18 PM
Low	Offline	Sign-ins from infected devices	76 of 78	1/17/2017 2:44 PM

7.9 Information Protection

To start with classification and labeling of document choose your battles. Define 1-2-3 labels for example: “High-Confidential Internal Only”, “Public” and “Internal Only”. It’s a good start without auto-labeling documents so people can learn how to protect their confidential data. In a later phase you can enable auto-labeling when a document is highly confidential for instance because there are credit-card numbers, personal information etc in this document. The activation of Information Protection could result from the fact that 1 million files are shared with external people. Or that you want to stop third-party applications, so company data stays safe in the environment.



Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with machines in your organization

52/100

Organization configuration score

Configuration score: 301 / 604

This score reflects the collective security configuration posture of your machines across OS, Application, Network, Accounts and Security Controls

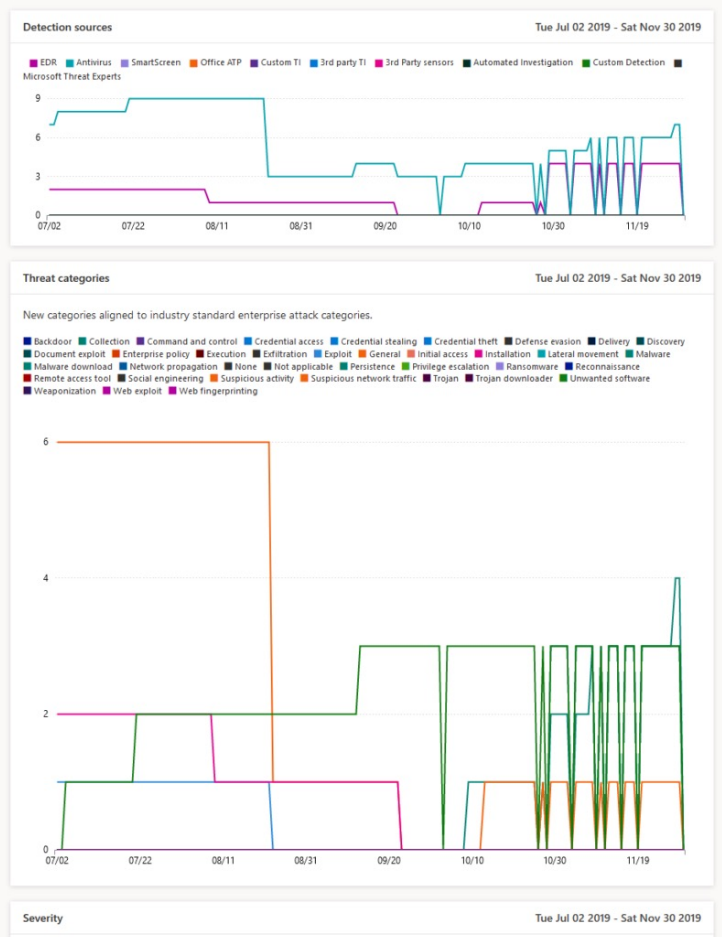
Application	18 / 78
OS	50 / 170
Network	42 / 88
Accounts	11 / 17
Security controls	180 / 251

7.10 Advanced Threat Protection

Work with Microsoft Defender Security Center (previous WDATP) will give you insights for Applications, OS, Network, Accounts, Security Controls + Give insights for Software patching, Top vulnerable software, Top exposed machines. Most reports are built-in and seamless integration is done in the Eco-system of Microsoft 365 E5.

7.11 Windows 10 Enterprise with modern approach

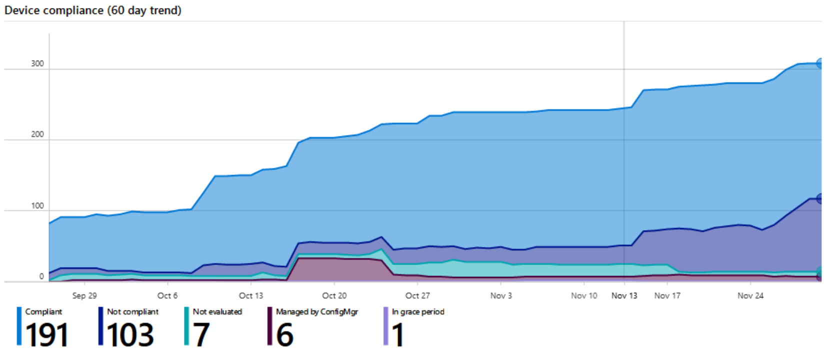
Windows 10: My personal favorite. I really love customers which did their homework and started using Windows 10 without policies, governance, Intune (for example), management solutions and now they are stuck in the patching & management of these systems. This is wrong!



Microsoft Windows 10: Windows 10 has been released to insiders in 2015. version. 1507 afterwards 1511, 1607, 1703,1709, 1803,1809,1903,1909. Microsoft did understand the pain of shifting from Windows XP to Windows 7, Windows 8 to 8.1 and Windows 10. And now they want you to work on these NEW versions in a different way.

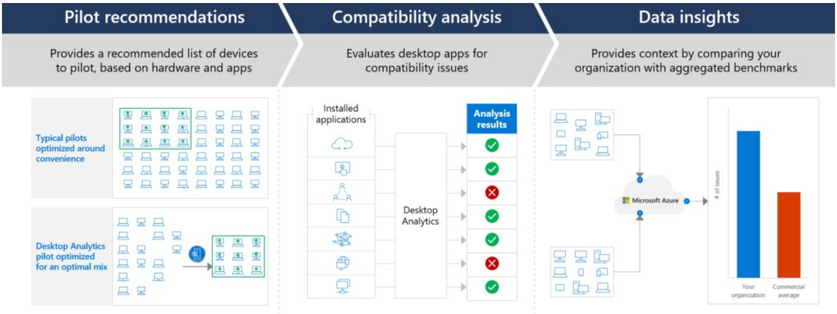
Microsoft's Windows 10 Enterprise: comes in the flavor of continuous improvement. And needs to be implemented in a service-model with automatic updates, rollouts, deployment, patching, updating, software requests (self-service) and even more!

Set compliance policies: Because of deep integrations you will be able to work on the compliance of the devices and grow to a recurrent update-model.



7.12 Desktop Analytics

Thanks to desktop analytics you will be able to evaluate the changes during updates such as software distribution and compatibility issues. You can bring your organization to a next level. In case you were afraid that automation took your job, think again. These things need huge attention!



Pilot recommendations

Provides a recommended list of devices to pilot, based on hardware and apps

Compatibility analysis

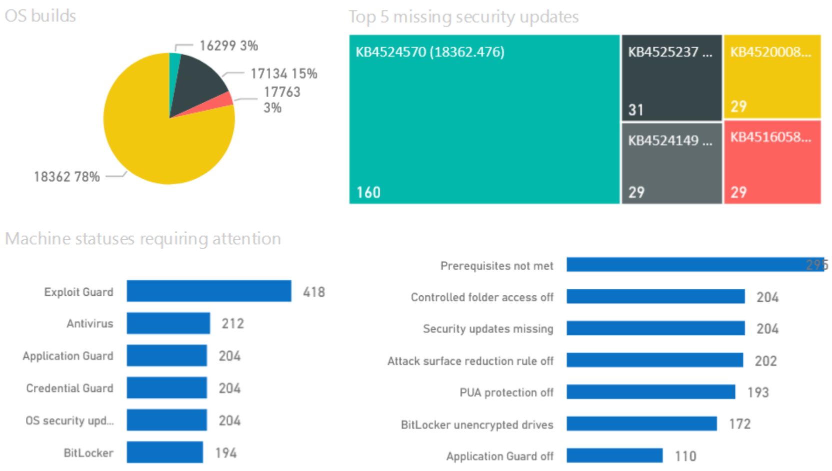
Evaluates desktop apps for compatibility issues

Data insights

Provides context by comparing your organization with aggregated benchmarks

7.13 Native Power BI Integration

Because of the rich Eco-system within Microsoft 365 everything can be measured. This report is default/ standard without any manipulation of Power-BI. I know it sounds not super relevant, but without insights one can't make decisions on facts. Features/services are changing every year. Be prepared. Start consolidation and start using standards to build on.



7.14 There is so much more

There is so much more if you go deep in Microsoft 365 E5. Microsoft is constantly updating their services to bring new solutions to the market which is super important to deliver to stay relevant.

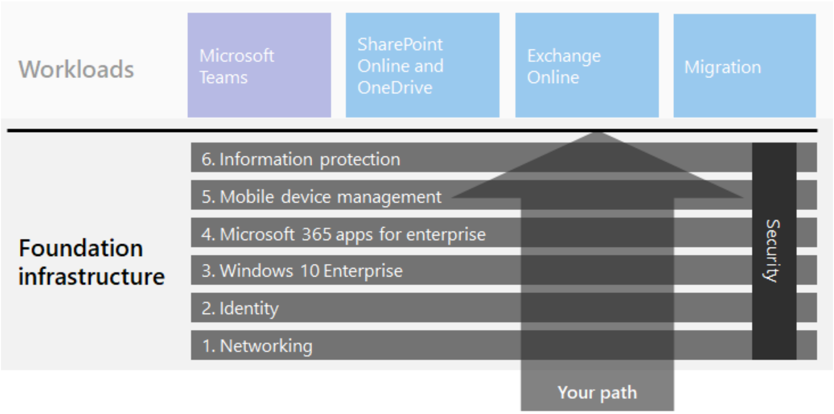
8.
Action plan to build a modern workplace.

8. Action plan to build a modern workplace.

8.1 Modern collaboration – for thriving your business

I've been around implementing on-premises solutions for collaboration as SharePoint infrastructure and global Exchange infrastructure. Fileservers, System Center and Server 2008 systems. Now, I don't believe organization should have this component anymore. The majority of the organizations are needing different solutions. I know that it's not wrong to hosts servers but from my opinion: Exchange, Microsoft Teams, Share-Point, OneDrive documents for collaboration should be used within the Cloud. Software-as-a-service has taken over in the fast world we are living.

Workloads: Microsoft Teams, SharePoint Online, Exchange Online and all other collaboration services.

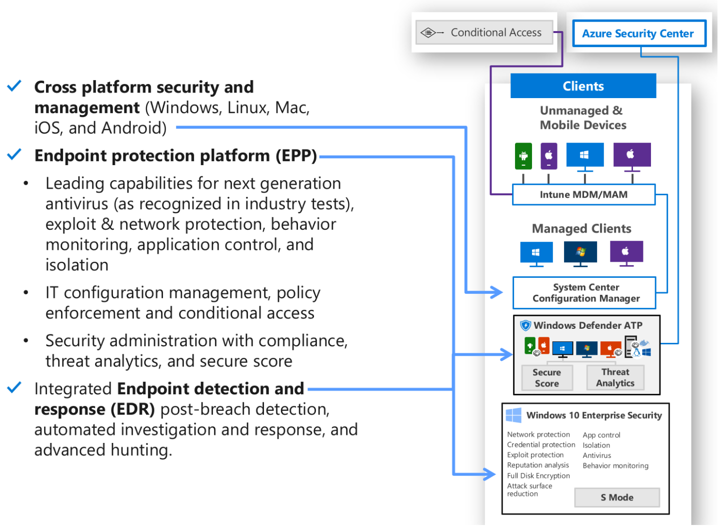

Workloads
Microsoft Teams
SharePoint Online and OneDrive
Exchange Online
Migration
Foundation infrastructure
6. Information protection
5. Mobile device management
4. Microsoft 365 apps for enterprise
3. Windows 10 Enterprise
2. Identity
1. Networking
Security
Your path

8.2 Endpoint management and protection

When building you endpoint management environment with Microsoft Endpoint manager integrated with the insights of all devices, Office 365, Active Directory and Azure you are able to use all rich capabilities to have a more secure environment.

When onboarding Cross platform security and management (Windows, Linux, Mac, iOS, and Android) you are more capable to protect and maintain the attack-surface for endpoints.

Workloads: Identity and endpoint management.



✓ **Cross platform security and management** (Windows, Linux, Mac, iOS, and Android)

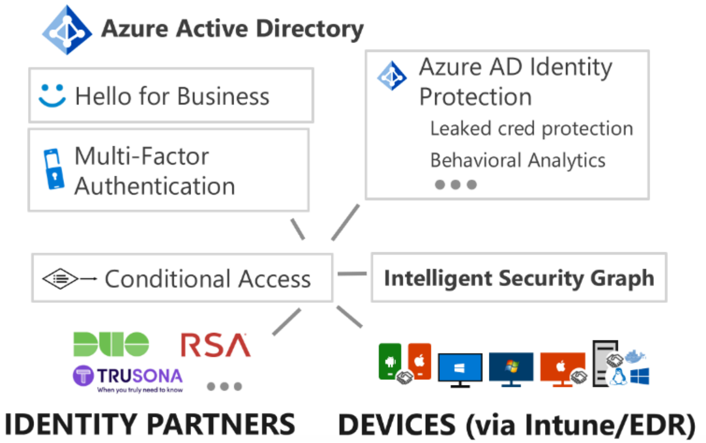
✓ **Endpoint protection platform (EPP)**

- Leading capabilities for next generation antivirus (as recognized in industry tests), exploit & network protection, behavior monitoring, application control, and isolation
- IT configuration management, policy enforcement and conditional access
- Security administration with compliance, threat analytics, and secure score

✓ Integrated **Endpoint detection and response (EDR)** post-breach detection, automated investigation and response, and advanced hunting.

8.3 Windows 10 Enterprise integrated in Microsoft 365

Windows 10/11 Enterprise is part of the cross-platform security and management layer as you can see in this figure below. Windows 10 deeply integrates in the Microsoft 365 stack.



To integrate deep into the Windows 10 workspace, identity and Access management should be included.

Workloads: Identity and endpoint management.

8.4 Roadmap to success – definition of ambition

When helping organizations towards Microsoft 365 and Azure I'm always trying to identify the core of the workplace and prioritize the business needs vs the technical 'things to do'.

As your organization is enabling more remote-working a decentral solution will rise. Talk with IT decision makers but more important business unit managers, HR management to create the ambition and roadmap where they want to grow towards – **together**.

In this stage it is important to define and write down what you like to achieve as for **example**: “Enable each worker with a collaboration solution to connect with every colleague” or, **“Create a digital workplace as a fundament to enable IT and insights everywhere”**.

In the next paragraph some practical steps from the field.

8.5 How to start to grow successfully to a modern workplace?

- What is the current ambition for modernization and how is it driven? Business, budget, IT, different...
- What’s the **current situation** of your ‘foundation **infrastructure**’? How are Identity, Windows 10 Enterprise, Microsoft 365 Apps, Mobile Device Management connected? Or how is infrastructure maintained at this moment and what is the plan for the future?
- What are the **biggest challenges of the workers** when it comes to their **digital work**? Do they have a lot of tools, are they trained? Are they frustrated for using a lot of tools? Would consolidation help? Or platforms with deeper integration.

When focusing on the modern workplace I’m always trying to investigate 3 aspects in the workplace:

- How are **people working** with technology at this moment? How are these systems provided to these people? Are they involved? Human-connected? Are they happy?

- **Technical assessment** of the infrastructure. Example: Exchange, Active Directory, Documents, real-time collaboration, video, audio call and different solutions. Also, great to know the weight of Microsoft 365 vs other platforms that are used by the workforce.
- How are new tech **chosen and used**; from a 'technical' perspective, by the IT-staff alone? Are there groups of people empowered to bring innovations and new systems to the table?

Mapping on the outcome we are identifying where the quick wins are. As for example; enablement of Endpoint manager or moving to Exchange online. And we are concluding together in which order we can migrate services to Microsoft 365 to achieve a business outcome.

Next to all these technicalities we always bring our adoption programs to the table. We will always advise to build a great team of business leaders, senior and middle management staff with their workers to have a mix of people involved to discuss the ambition. The impact of human connection and involvement is still underestimated from my opinion.

Last but not least. From an implementation perspective and also people perspective; training and technical implementation should come hand-in-hand. Therefore, we have built a great standard-set of onboardings programs to go fast but pragmatic.

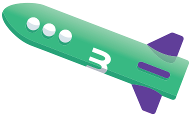
As you can read there are great adventures ahead when it comes to the modern workplace and we at Wortell can help you face these challenges head on! Contact us for more information about our solutions for Microsoft 365, Azure and Microsoft Security and how we can guide you to your ideal situation.

Thank you for reading!

Jasper

9.
Work

9. Work.



Wortell offers a modern, compliant and secure modern workplace as a standardized solution for a fixed price per employee per month. We will manage everything from Windows 10 and Intune to Office 365. The workplace will always be up to date and compliant with applicable laws and regulations. Standardization and almost fully automated management ensure that that's something you can rely on!

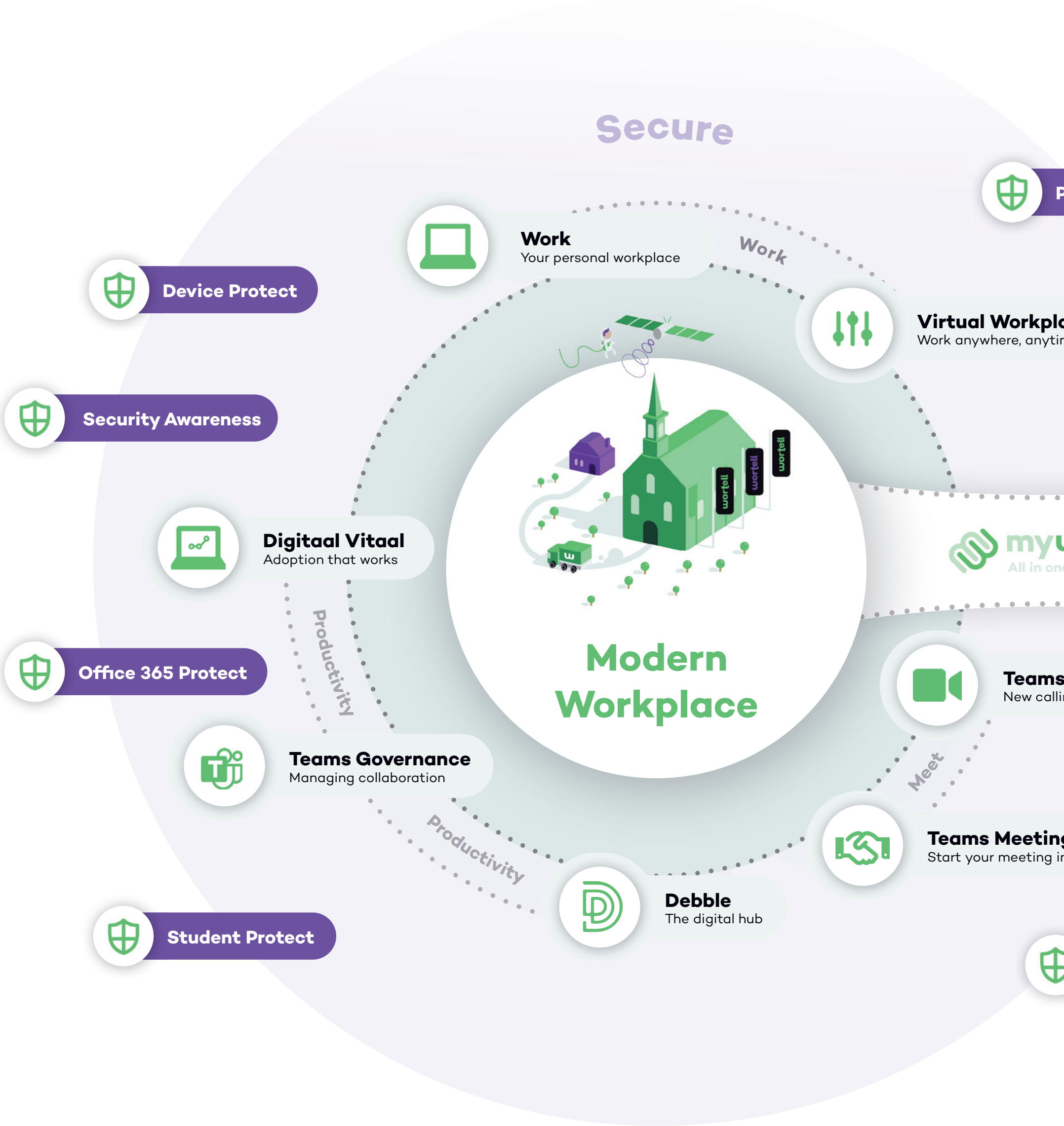
During and after the implementation, we will use an effective adoption approach to make sure your employees embrace the modern workplace. They can also fall back on our digital personal trainer and coach, JIM, who is always included in the product.

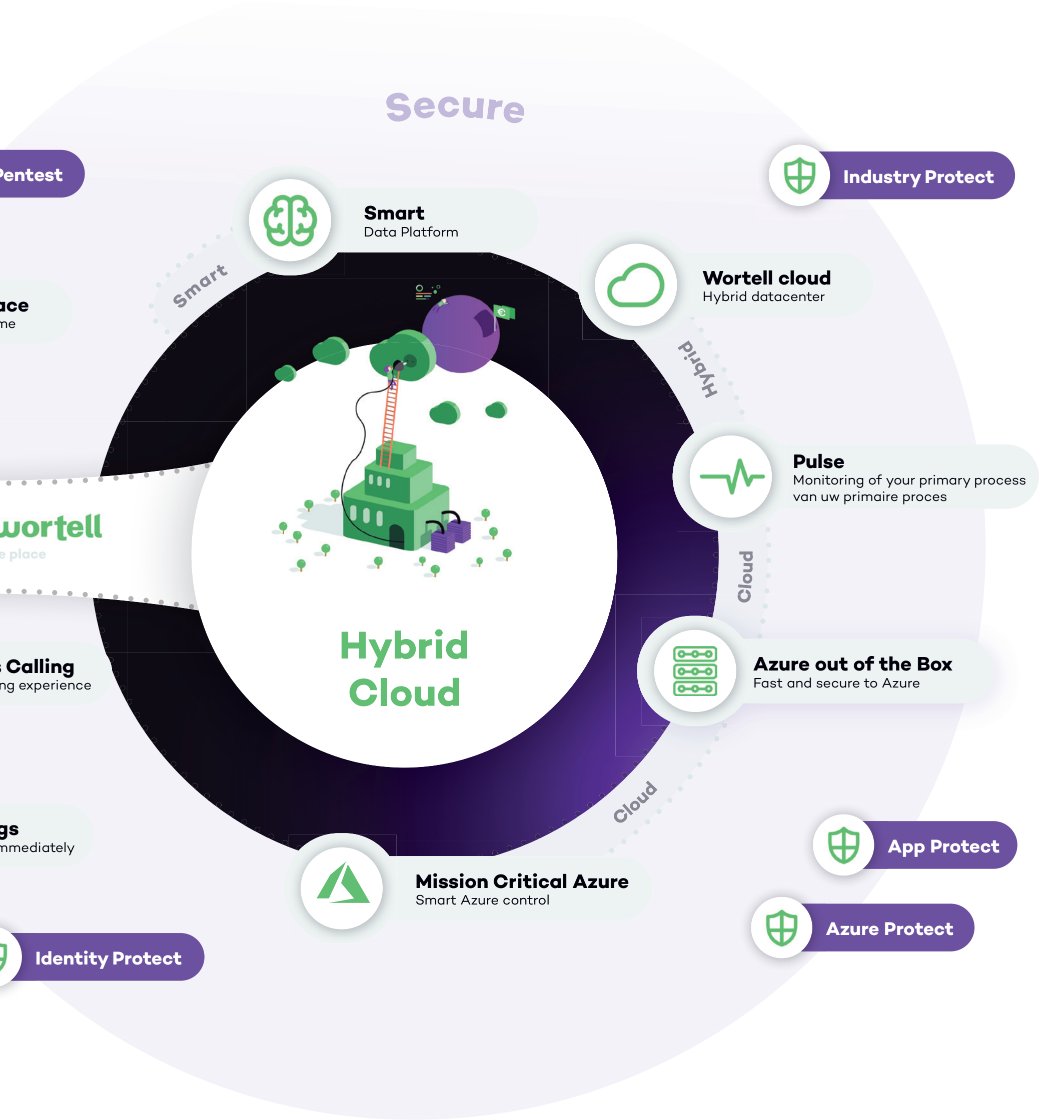
Self-service through MyWORK

Do you expect an auditor's visit? Or do you require insight into where your workplace currently stands? Through the MyWORK portal, you will find all the information you need in a trice. Key users and end users can also access this self-service portal, where they're able to add functionalities or applications to the workplace without having to call in the help of Wortell or the IT department.

wortell
wortell
wortell

We empower people.





Secure

Pentest

Smart
Data Platform

Industry Protect

Smart

Wortell cloud
Hybrid datacenter

ace
me

Hybrid

Pulse
Monitoring of your primary process
van uw primaire proces

wortell
e place

Cloud

Hybrid
Cloud

Azure out of the Box
Fast and secure to Azure

Calling
ng experience

Cloud

gs
mmediately

App Protect

Mission Critical Azure
Smart Azure control

Azure Protect

Identity Protect

wortell

We empower people.

wortell