**HOW TO BUILD YOUR ZERO TRUST MODERN WORKPLACE WITH MICROSOFT 365**

Thank you so much for reading my blog about: **How to build your modern workplace with Microsoft 365**. In this article I’ve written an high-level approach of an implementation and shift from a more traditional organization towards a cloud focused organization. I would love to receive feedback in in the comment, on [Linkedin](https://www.linkedin.com/in/jasperbernaers/)or [Twitter](https://twitter.com/Jasper_be). Also read: [**The value of Microsoft 365 E3 and E5.**](https://jasperbernaers.com/the-value-of-microsoft-365-e3-or-e5/)

This blog is describing the strategic, high-level possibilities of Microsoft 365. The [next blog will be a high-level technical implementation.](https://jasperbernaers.com/technical-high-level-modern-workplace-implementation-with-m365-e3-e5/)

**Strategy and vision**

Welcome in 2020. The world has changed since the last pandemic. Organizations are struggling to anticipate better on their workforce to help and achieve their ultimate goals.

To collaborate better, to get in contact different than before a more modern approach is necessary – change is required. I don’t want to go to deep in the fact that it is becoming a huge challenge for CIO’s and IT Manager since the world has shifted into a new era. Working different has become a new standard. And the change driver is from the outside towards inside. It is happening – there is no way not to accept the signals. There is no way, not to change.

When mapping these challenges on the real technological ‘needs’ I’ve summed up some topics that will come back in my article, later. The main technological challenges are:

* **To connect people** to collaborate in a different way with new technical possibilities – Keeping in mind that the experience needs to be great. It should be simple. Transparent. Team driven, no individuality.
* **To use proven standards that do work** – because they are used in multiple organizations. The slowness of not believing these standards and references and going the own way is killing organizations. This results in slow implementation speed – lack of confidence and trust which results in over thinking. And conclusion: failing.
* **To provide the right tools that do work for organizations**– in a modern world – without the fence of physical locations and more important with the same security level as in the early on-premise days.
* **To be fast enough** and accelerate your business goals. Timing = everything.
* **To get you security maturity in order,** better, safer, to grow to a technical safer workplace – this is more important than ever. If you see the cyber Risk trends growing, somethings needs to change.

Companies are working different than before. And I trully believe that the one that is most adaptable to change do survive.

***It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change.***

**The traditional corporate infrastructure is isolated of the outside world**

As you can see in this beautiful picture that’s is brought by Microsoft in the [zero-trust concept](https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft) organization did build great solutions in their datacenters on their premises. In their decentralized redundant datacenters with everything in place to have their DRP and failover working great. I’m not bashing on smart people which did a great job fixing these massive complex integration to keep everything running 24/7, in their de-central service centers / data centers.

Diagram

Description automatically generated

The problem is, the solution is… As I’ve mentioned in my last point. Organizations did a great job, on their premises to get everything working great.

Disruptive 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’ of Infrastructure on premises. Software-as-a-Service (SaaS) solutions that were isolated from these corporate environments with plug and play capabilities to most important leverage solutions for these organizations – and this is the most important aspect of it all. Solutions for organizations, to achieve more. The get to the ultimate goals of these organizations. Non technical driven scenario’s, business case and business scenario’s. I think we are somewhat naïf not understanding why disruptive came. It is mainly because we were not able to adapt on changes required to make our organizations more modern. With high speed implementation. Image a new Office 365 customer in a cloud scenario. With: Exchange, Sharepoint, Teams, mobile device management. They can start after some hours of implementation. Image this setup on- premises. How long will it take? Perspective = everything.

**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.

Chart, diagram

Description automatically generated

Microsoft didn’t invented the layered approach when it comes to: Identity, Devices, Services, Data and Network. It’s no new model nor real solution that fixes any problem. No, it’s 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. And 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. The right conclusion: Layered approach.

**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 came disruptive like BPOS, Office 365 and we did integrated our current infrastructure with Identity federation solutions as 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](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect). A modern tool that helps extending your current on-premise Active directory to Azure Active Directory. But we didn’t thought 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 a 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 platform. Building blocks. Easier for activations as for example: Azure AD Security Defaults. Maximum value, less complexity faster implementation speed.

Diagram

Description automatically generated

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

Before 2020 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 shifted in the Office 365 landscape. For example:

* Fileservers became -> OneDrive, SharePoint or Microsoft Teams
* SharePoint on-premise -> Hybrid -> SharePoint Online
* Mail/Exchange on-premises -> 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)

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 change! Old legacy, phase it out, migrate to different solutions. Focus long-term.

Table

Description automatically generated

**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. Were staged by System-Center Configuration Manager in a on-premise solution. And are now brought in a hybrid deployment with [Microsoft EndPoint Manager](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview).

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 implement, during Covid-19 the change of update mechanisms from SCCM towards Endpoint Manager.

Graphical user interface

Description automatically generated

In this great overview you see on the left the integration of the current Active-Directory environment towards Azure Active Directory. In the right you see future state building blocks that needs 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 scenario’s 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 became less important compared to security implementations and improvements.

* **The first reason:** **The configuration and implementation is easy.** Not because I’m lazy to implement more complex solutions but the create simplified standard solutions to manage your Windows 10 Devices is 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 protection 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 full-cloud, 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)
* **Fifth reason**: **No hybrid complexity,** easier staging with Windows Autopilot. Staging from anywhere. Not possible in hybrid scenario’s, at the moment. It’s announced will be possible soon.
* **Sixth 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 touchable factor. There are more capabilities easier to implement. Long-term is the real reason.

A picture containing diagram

Description automatically generated

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

* When your not in a hurry moving to full-cloud. And for example 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. Its better to make the invest in modern tools compared to well know configuration manager.
* When you have 20 language packs and custom scripts. Sometimes hard decisions needs to be made to be more flexible in a later stadium. Again, Strategic decision.

**Services, servers and infrastructure**

It’s al 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 integration with active-directory. Next to Security TCO is important. Did you know that we spend a lot of our time doing core-infrastructure task to keep everything running. It’s so critical infrastructure. Do we really want to keep on working and supporting this infrastructure when there are other options? It’s 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.

Chart

Description automatically generated

The next diagram shows the responsibilities – import for knowing the opportunity for engineers, architects and the impact on these people. Next to the workload and impact the technology is probably more important.

Diagram

Description automatically generated with medium confidence

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

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

Diagram

Description automatically generated

**Data (documents)**

Data maturity. automatic processing. Automation,. You get the point. (document)data is crucial and needs protection. 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.. We need a consolidated approach to fix 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 of 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” maybe because we are having less smart people really understanding what we are doing.

* **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 tech goes beyond the tool itself.
* **Migrate**personal **documents**to OneDrive, Organizational document to SharePoint of 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 an classification or at least insights on confidential data. We lack data-control. Not even ‘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 document when the risk of data-leakage is valid. Cloud App Security will not 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** is hard. But it’s even harder if you also have on-premises resources and non-controlled instances. The pro’s of only O365 is you can deliver actionable insights.

**Network**

I’m not a network specialist. I don’t know a thing of networking. But what I do now is that because of this ‘gap’ of IT-Pro’s to opportunity of hackers will rise. Because of the unknown facts. If you are able to shift all workloads to Microsoft 365 the network part, and the network-security will become less important. When it comes to information breaches, and core-infrastructure is gone on the on-premises. Every organization needs stable network, shaping, priorities and all other things to regulate network infrastructure. It is super important. But, we need to stop trusting our own networks as much as we did, before. Because the silo walls are gone. The crucial organization data did shifted to somewhere else.

Why should we even make a more trusted inside network than outside over VPN or private connections?

Table

Description automatically generated with medium confidence

**Strategic modern workplace decisions**

Strategic long-term definitions are important to set milestones to grow to a real modern workplace. Most of the time we are delivering workplace optimizations for 20% of the workplace – of the possibilities and the needs. Only modern management for example.

* **Shifting al or our traditional infrastructure to Azure**, Microsoft 365 is crucial for the long-term. For future-proof [architecture](https://docs.microsoft.com/en-us/office365/enterprise/microsoft-cloud-it-architecture-resources).
* **Modern Management is a part of a workplace**. For just only managing your assets, devices, updates, applications and deployment. But we are making this the import part. It’s the easy part. maybe in the near future Microsoft will deliver end-to-end solutions for deployment and management of devices. I hope they will. Probably we will complain of Microsoft taking over. And we are not willing to see the opportunity of the broad workplace.
* **Security baselines** became important to get easier packages with a big value, low-cost, maximum impact. Building blocks to implement to get your organization on a high(er) security level.
* Consolidation and migration to Microsoft 365 gives control to start with **Unified Classification of documents** and rich integration with for example PowerPlatfrom. It’s a tremendous opportunity to see how data is moving thought your workplace. And it creates insights to get things in order.
* Real **communication and collaboration** is possible from anywhere if you brought all services from on-premises to Microsoft 365. Example: Using Teams with an on-premise exchange? What’s the strategy for that? And this brings me to the start of the article.

**There is no room for traditional workloads when your strategy is to work and invest in Security optimizations. There is no room for traditional Exchange, SharePoint and fileservers when you want to be a flexible and cloud company**.

We have seen the world changing the last 3 months. Maybe we will turn back to where we were. The choice now is:

* Would you be the company that is prepared for next trends of working from anywhere – with a future proof ready architecture. to build on. To grow security, data maturity and easiness of future integration and implementations?
* Would you go back, and use the old-tech? Until your organization is irrelevant because someone will change faster someday.

***It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change.***