**[Get Started With Zero Trust in Microsoft 365](https://danielchronlund.com/2021/01/13/how-to-get-started-with-zero-trust-in-microsoft-365/)**

Before getting to the topic of this post, I just wanted to talk a little bit about my expectations for 2021. This is my first blog post in 2021 and I feel that this year will be filled with inspiration and exciting new projects. I’m both proud and humble that I’ve just received my first [Microsoft MVP](https://mvp.microsoft.com/en-us/PublicProfile/5004116?fullName=Daniel%20Chronlund) title. I’m now an **Enterprise Mobility MVP** which includes interesting products like Azure AD and Microsoft Endpoint Manager. Please, feel free to reach out to me if you want to discuss anything Microsoft 365 security related. Of course, I will continue to provide tools, tips, and thoughts for the IT pro community through this blog, and I also have a couple of other interesting new things coming up in the following months, so stay tuned!

Let’s get down to business! 2021 will also be an extremely security focused year. COVID-19 boosted the digital transformation, but it also boosted cyber crime. Attackers are moving their focus to the cloud and we all need to implement better security models. Zero Trust is the one you’ve all heard about, and there’s a good reason for that. This method of doing security can be applied both on-prem and in the cloud, and Microsoft 365 was built to provide this security model for you, with the right configuration of course.

In this blog post I will explain what Zero Trust is and provide links to some of the best Microsoft Zero Trust resources out there. Use them to learn, to get started, or to complete your Zero Trust journey. I believe that this is crucial for every organisation out there! Good luck on your journey!

*A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements. Each of these is a source of signal, a control plane for enforcement, and a critical resource to be defended.*

**The Microsoft Zero Trust Deployment Center**

**The Three Principles of Zero Trust**

These three guiding principles explains the concept of Zero Trust and what we need to do to provide a more modern security model.

* **Verify explicitly**
* **Use least privileged access**
* **Assume breach**

**Verify explicitly** means that we need to always authenticate and authorise based on all available data points. Don’t trust a user or a device, verify that it’s what it claims to be! **Use least privileged access** means that we must limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection. Finally, **Assume breach** means that we must minimise blast radius and segment access. It should be difficult for an intruder to move laterally throughout the environment. Also, verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defences.

You might have seen the well known **Integrated Microsoft Zero Trust Model** diagram. This is it, with a couple of my own additions in green and purple to actually explain what I believe should be the products and services used to implement the three different principles in the Zero Trust model.

Diagram

Description automatically generated

When we can do all three of these principles, throughout our entire digital estate, then we have reached Zero Trust. However, every part that we implement increases our security posture. Zero Trust is a journey, for some organizations, a long one. Everything we can do raises the bar, and that’s the goal!

**Zero Trust Assessment Tool**

The [Microsoft Zero Trust Assessment Tool](https://info.microsoft.com/ww-landing-Zero-Trust-Assessment.html) is a wizard driven questionnaire that answers the question, where are we today? You answer questions in different areas like identity, device, data and infrastructure to assess where you are on your Zero Trust journey. I’ve been using this tool in customer workshops for almost a year now and I think it’s a great way to get started and to understand what Microsoft means by Zero Trust. Please start of by going through this assessment!

**Zero Trust Business Plan (this is for your boss)**

Microsoft provides a [great business guide](https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4JAsW) to implementing Zero Trust. It explains why Zero Trust is a requirement for securing the rapid digital transformation that is happening right now. Make no mistake that the transformation will speed up even more the next couple of years. Everyone is going to the cloud, and it’s happening right now, no matter if you like it or not. Use this material to sell the concept of Zero Trust to the leadership in your organisation. Basically, this is for your boss! Here are some business arguments (not so security related) mentioned in the guide:

* Support work from anywhere at any time.
* Enable secure and rapid cloud migration.
* Realise cost savings through simplification of the security stack.

The Zero Trust business plan teaches us about three different phases of the journey. Each phase includes guidance, best practices, resources, and tools to help you drive your own implementation. The phases are **Plan**, **Implement**, and **Measure**. It explains why each phase is important, and how to execute it. Use this resource to create your own Zero Trust business plan!

**Microsoft Zero Trust Deployment Center**

Now it’s time to get down to business! The [Microsoft Zero Trust Deployment Center](https://docs.microsoft.com/en-us/security/zero-trust/) is the one-stop-shop for all Microsoft Zero Trust content. It’s is divided by area and explains why and how you should implement certain security features and products to enable Zero Trust. The different areas are:

* Secure identity with Zero Trust
* Secure endpoints with Zero Trust
* Secure applications with Zero Trust
* Secure data with Zero Trust
* Secure infrastructure with Zero Trust
* Secure networks with Zero Trust
* Visibility, automation, and orchestration with Zero Trust

It basically provides you with a complete road map/checklist for each area and with this you will save many hours of planning your Zero Trust journey. I strongly encourage everyone who’s working with security in Microsoft 365, and in Microsoft products overall, to read the guides in the Zero Trust Deployment Center. It’s an eye opener if you haven’t read up on Zero Trust before!

**Final Thougts**

There is a good reason why I’m starting this year with this blog post. This is what I’ll be working on with my customers in 2021, and so should you! Zero Trust is the future of cloud security and it is a great way of making it really hard for attackers to reach their goals. I also want to mention **password-less** as this also will be an important topic this year, and it is an important part of increasing the security around your identities.

Good luck on your Zero Trust journey and I wish you all the best in 2021!