eSHARE

How Zero Trust Creates Trusted Collaboration

White Paper

Mark Cassetta

Introduction

The need for organizations to shift to Trusted Collaboration is greater than ever before. The pace of innovation and service expectations is one that demands organizations to operate at a velocity that is unprecedented. Compounding this is the adoption of Generative AI to both accelerate how people work (e.g. Microsoft Copilot) as well as deliver products and services.

Without trust between knowledge workers and security, the business will fail to meet the incredible expectations that have been placed on it. The irony is that in order to deliver on Trusted Collaboration, the organization must adopt the principles of Zero Trust.

The Zero Trust Tipping Point

Enterprise security has been on a quest to adopt Zero Trust principles for more than a decade. While the initial principles of Zero Trust date back to the Jericho forums in the early 2000's, adoption was greatly accelerated and arguably tipped, when the workforce went completely remote in 2020. Principles such as continuous, contextual as well as risk-based policy enforcement, that would eliminate standing privilege, were required for secure remote access.

The accelerated adoption of Zero Trust principles was driven by a complete shift in how organizations would collaborate. Before 2020 modern collaboration platforms (e.g. Microsoft 365) fueled by link-based sharing were being adopted, but there was no compelling event for enterprises to really think about how collaboration should mature. Of course there were visions, but most of the market saw modern collaboration as a "nice to have" instead of a "need". Fast forward to March 2020 when the world went remote, organizations had no choice but to embrace and promote modern collaboration platforms (with Microsoft 365 leading the charge for enterprises), if nothing else for business continuity during a global pandemic. Stories of large complex, 100,000 person organizations deploying Microsoft 365 in weeks, when they originally planned for it to be years, were common.

As CIOs tried to figure out how to adopt Microsoft 365 at a rapid pace, IAM leads were given everything they needed to ensure people could log in securely without a VPN. While identity was fast tracked to enable remote access to Microsoft 365, data security lifted and shifted their existing strategies to try and shoehorn them into modern collaboration. Of course, this was the right thing to do at the time to keep the lights on, but forcing users to use legacy data security approaches/tools for link-based sharing quickly became inefficient and insecure.

Old data security products and processes were designed for a collaboration model that revolved around the sharing of a file. Modern collaboration is centered around the sharing of a link where Zero Trust policies need to be applied at both the time of sharing as well as the time of access for them to be effective.

Zero Trust *NOT* in the Flow of Work

Over the last few years, a lot has been written about getting into a flow state to create great work. That "flow state" is very precious and forcing knowledge workers to exit that flow and context switch when trying to get work done is frustrating.

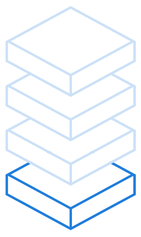
Unfortunately, this is what many legacy approaches to data security forced users to do when attempting to secure Microsoft 365. For example, forcing users into a third-party process to create a ticket, which could take days to complete, simply to share a file externally became a reality for many organizations. This was not only frustrating, but very expensive given the unnecessary third-party process and capacity required to manage it. However, this was what organizations felt they needed to achieve their compliance and security requirements through the lens of Zero Trust principles. While not intentional, all security did was perpetuate a reputation of not enabling the business and creating a frustrating user experience which failed to create a Trusted Collaboration experience.

Zero Trust in the Flow of Work

So how does an organization enable knowledge workers to stay in the flow while enforcing Zero Trust principles? It starts by deploying a data centric security strategy, which includes:

Keeping the data in the Microsoft 365 tenant: central to data centric security is letting users share natively with links (instead of forcing any kind of download) so that the data never has to leave the Microsoft 365 tenant. The moment the data leaves the tenant, the ability to apply the principles of Zero Trust, such as least privilege, disappears.

Share based on context (e.g. sensitivity): creating effective least privilege policies that minimize user friction through automation is dependent on being able to leverage file and user attributes (context) to streamline policy decisions. The level of context available to will vary according to the organization's maturity:

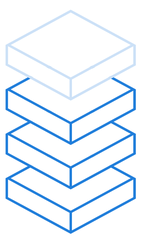


Level 0 – no sensitivity labels:

If the organization has yet to adopt any kind of sensitivity label, simply allowing the user to make a secure sharing decision themselves within the Microsoft 365 platform is a good start.

Level 1 – container labels:

The organization may not be ready for a user driven labeling strategy, but by labeling containers and SharePoint sites, context starts to become more available allowing for the sharing policies to become automated.



Level 2 – file and email labels:

As the organization starts to mature its labeling strategy and users can start self-selecting sensitivity, then the context and the quality of the secure sharing decision increases.

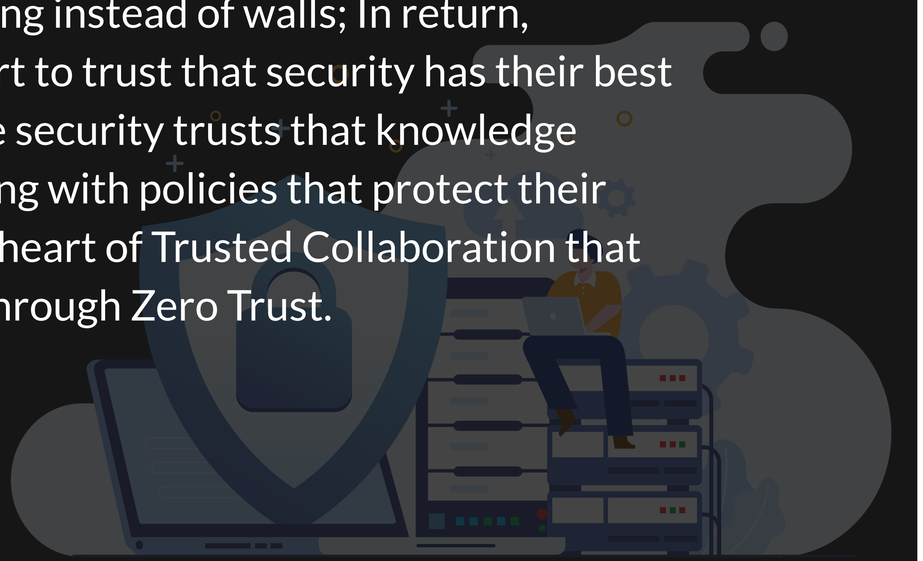
Level 3 –organizational signals:

Beyond labels, the enterprise can start to bring richer context into the sharing decision that is unique to its environment. For example, pulling recipient attributes from a central system (e.g. CRM, HR, ITSM) to determine the type of sharing policy helps to further offload the sharing decision from the knowledge worker.

Apply policies at the time of access: applying Zero Trust principles in the flow of work is not just at the time of creation, but also every time a recipient goes to access the link. Just because the recipient had access two weeks ago, does not mean they should get access today. Time of access policies are central to reducing standing privilege and ensuring only the minimum amount of access is required while still enabling collaboration.

Deploy Guardrails, Not Walls

By deploying a data centric security strategy with Zero Trust principles, the organization is choosing to put guardrails around link-based sharing instead of walls; In return, knowledge workers start to trust that security has their best intentions in mind while security trusts that knowledge workers are collaborating with policies that protect their information. This is the heart of Trusted Collaboration that is ultimately achieved through Zero Trust.



Unlock the Power of Trusted Collaboration

Zero Trust is the foundation of secure, compliant, and efficient collaboration. Contact us to discover how eSHARE's solutions enable seamless data sharing while aligning with Zero Trust principles.

Mark Cassetta
Chief Product Officer
at eSHARE

Linkedin
info@eshare.com
www.eshare.com