

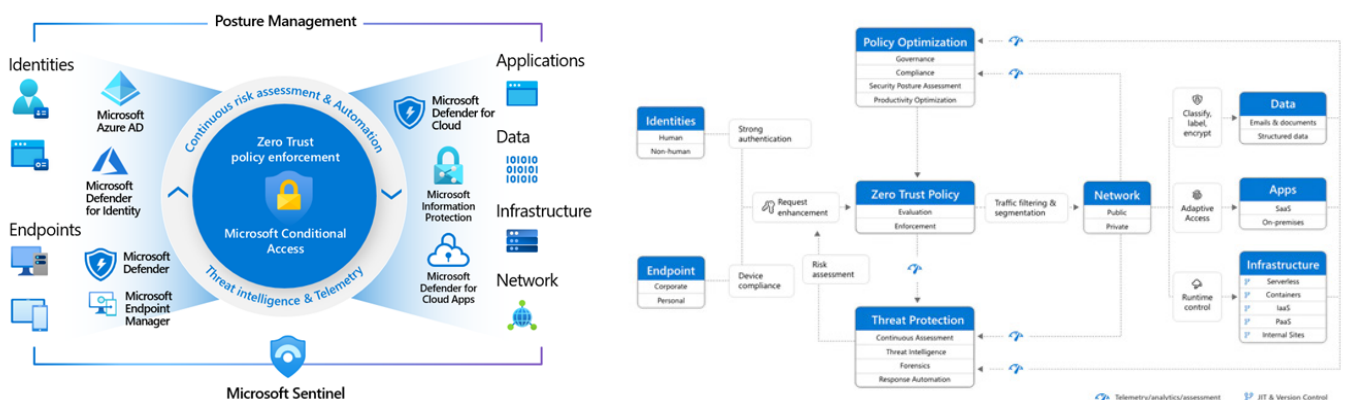
# Zero Trust - der Marathon für IT-Challenges

**Die Arbeitswelt wird immer agiler und ist so einer Vielzahl an Angriffsvektoren ausgesetzt. Zum Schutz Ihrer digitalen Daten, dem Gold des 21. Jahrhunderts, ist eine Zero Trust Strategie unabdingbar.**

Das Grundprinzip der Strategie bedeutet, dass Nichts und Niemanden vertraut wird und permanent Challenges (Prüfungen) bestanden werden müssen. So wird eine kontinuierliche Verifizierung aller Transaktionen gewährleistet. Zusammen mit einer geringst möglichen Privilegierung und Echtzeit-Erkennung sowie -Reaktion auf Bedrohungen ermöglicht dieser proaktive Ansatz über alle digitalen Ebenen Sicherheit für Ihre digitalen Daten.

<p><b>EXPLIZITE PRÜFUNG</b></p> <p>Überprüfung aller verfügbaren Datenpunkte, einschließlich:</p> <ul style="list-style-type: none"> <li>• Benutzeridentität und Standort</li> <li>• Gerätezustand</li> <li>• Dienst- oder Arbeitslastkontext</li> <li>• Datenklassifizierung</li> <li>• Anomalien</li> </ul>	<p><b>ZUGRIFF MIT GERINGSTEN RECHTEN VERWENDEN</b></p> <p>Um sowohl Daten als auch Produktivität zu sichern, den Benutzerzugriff begrenzen durch</p> <ul style="list-style-type: none"> <li>• Just-in-time (JIT)</li> <li>• Just-enough-access (JEA)</li> <li>• Risikobasierte adaptive Richtlinien</li> <li>• Schutz der Daten vor unzulässigen Vektoren</li> </ul>	<p><b>ANNAHME EINES VERSTOSSES</b></p> <p>Minimierung des Einbruchradius und Verhinderung vertikaler Angriffe durch</p> <ul style="list-style-type: none"> <li>• Segmentierung des Zugriffs nach Netzwerk, Benutzer, Geräten und App-Awareness.</li> <li>• End-2-End-Verschlüsselung aller Sitzungen.</li> <li>• Verwendung von Analysen zur Erkennung von Bedrohungen und zum Aufzeigen der Sicherheitslage und Verbesserung der Abwehrmaßnahmen</li> </ul>
---	--	--

## Microsoft Zero Trust Capabilities



**Sind Sie bereit für den Marathon? Wir sind Ihr Laufpartner!**



**Samir Colovic**  
samir.colovic@orbit.de  
+49 151 58037804