Cyber Threat Exchange Liechtenstein
26. September 2023

AVANTEC
Competence. Security. Trust.

Einfluss des Zero-Trust-Ansatzes auf die Cyber-Abwehr-Fähigkeiten

Peter Hämmerli, Senior Presales Engineer, AVANTEC
September 2023

AVANTEC
Competence. Security. Trust.

DNA der Denkweise für Security-Experten

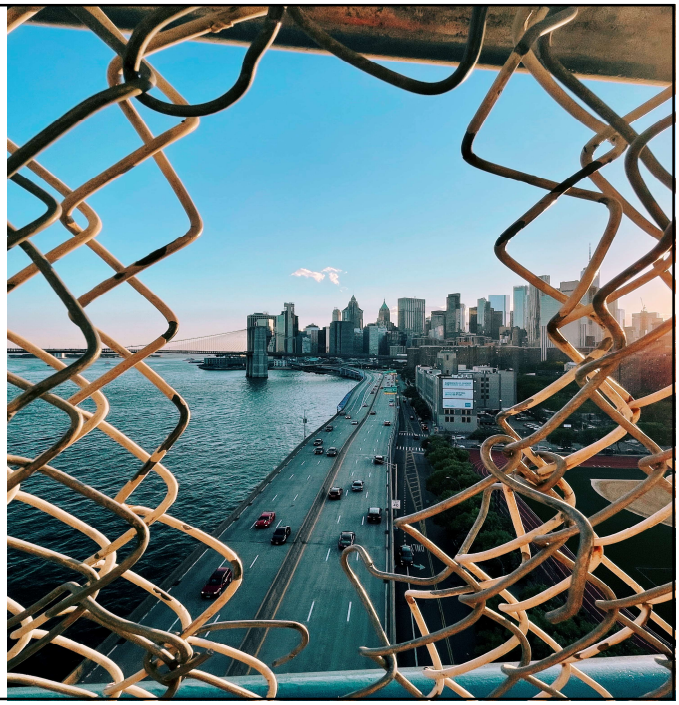
AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Assume a breach!

Gehen Sie davon aus, dass Ihre Organisation jederzeit angegriffen werden kann. Auch gerade jetzt.

Es gibt keinen 100%-Schutz!



You are under Attack!

Gehen Sie davon aus, dass nicht alle Sicherheitsvorgaben eingehalten wurden und dass die «Angreifer» bereits in Ihrer Domäne sind, resp. sich bereits auf Ihren Systemen eingenistet haben.

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Die Cyber-Security-Welt verändert sich stetig

Gestern

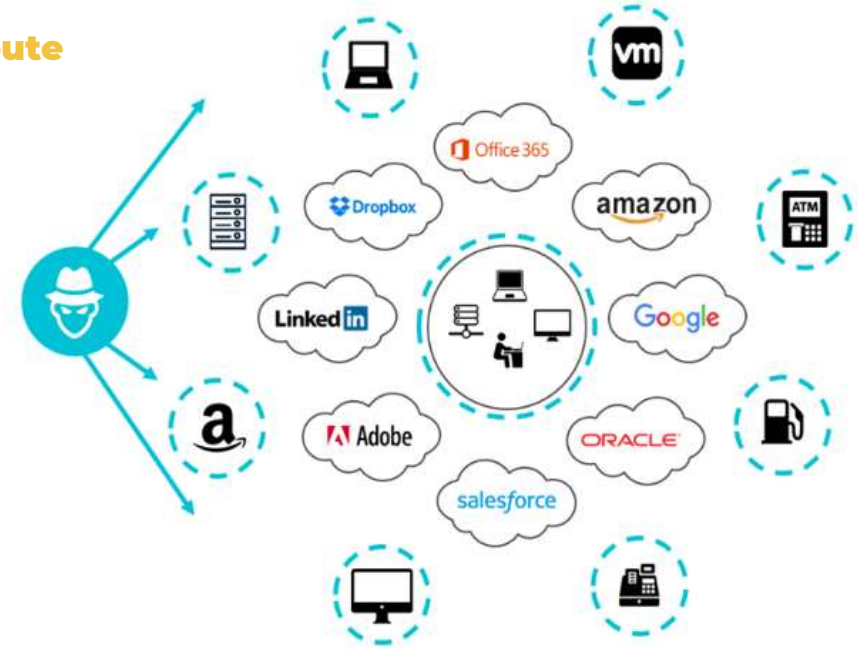
Traditionell haben alle Unternehmen auf Firewalls als wichtigsten Netzwerkschutz gesetzt. Dabei galt der Ansatz, dass der Angreifer immer über den Perimeter (die Firewall) kommen wird.

Es galt auch, dass sämtliche Nutzer und Anwendungen innerhalb der eigenen Domäne als vertrauenswürdig einzustufen waren.

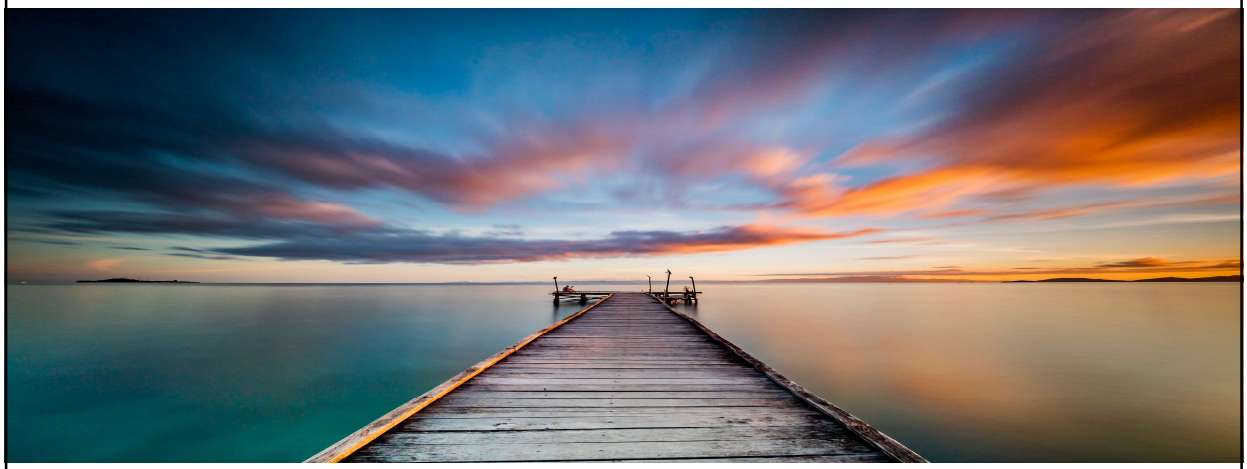
Diesen Ansatz gilt es zu überdenken.
Er bringt bei heutiger Bedrohungslage keinen ausreichenden Schutz!

Cyber Threat Exchange Liechtenstein
26. September 2023

Heute



AVANTEC
Competence. Security. Trust.



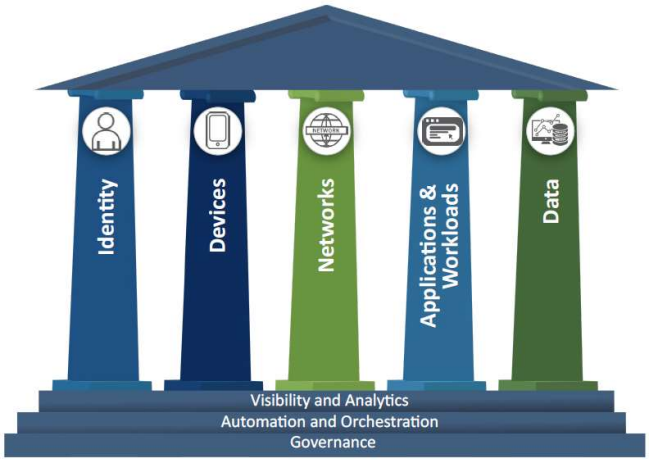
Paradigmenwechsel

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

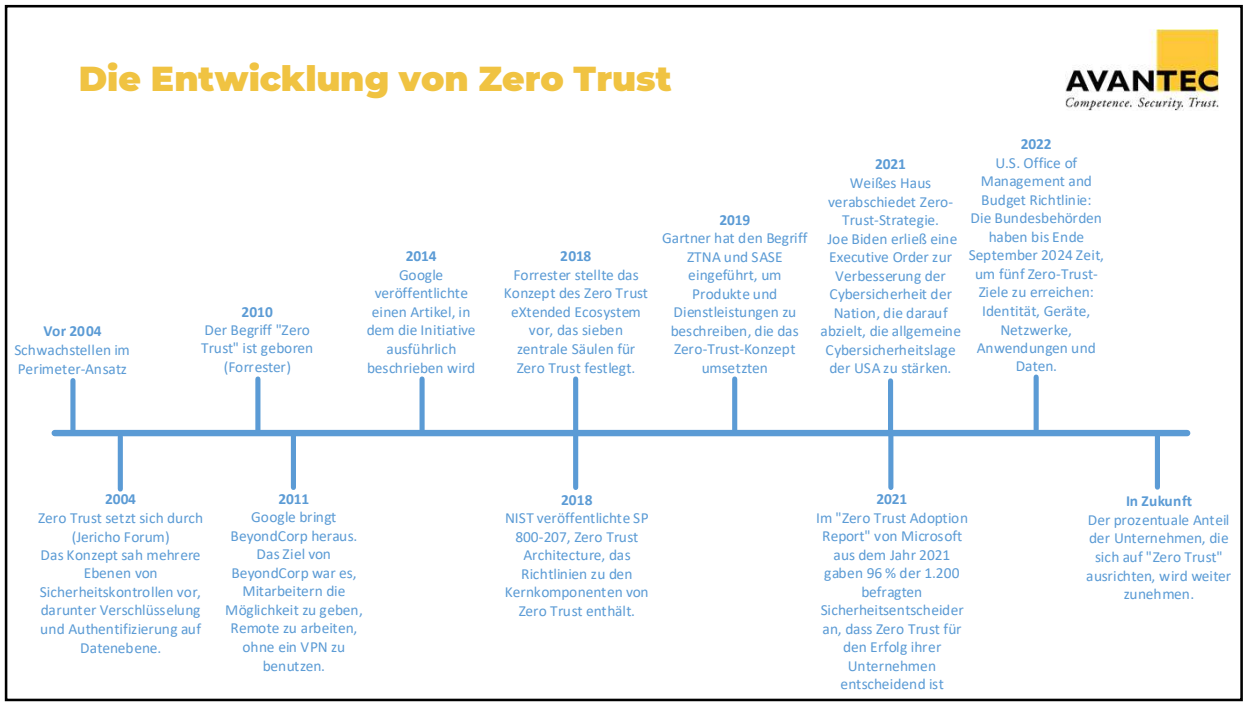
Trust no one or anything – and always verify

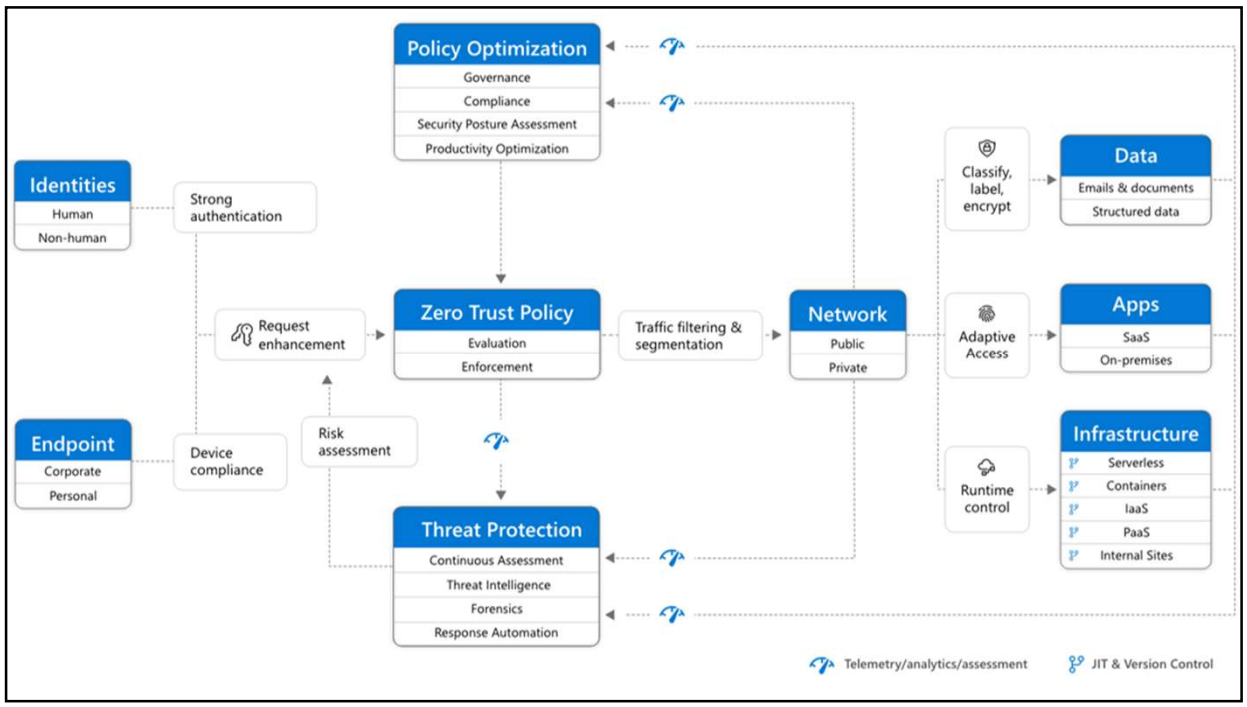
Die Säulen von Zero Trust



Cyber Security and Infrastructure Security Agency, USA

Cyber Threat Exchange Liechtenstein
26. September 2023





AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Wo greift der Zero-Trust-Ansatz bei der Cyber-Abwehr?

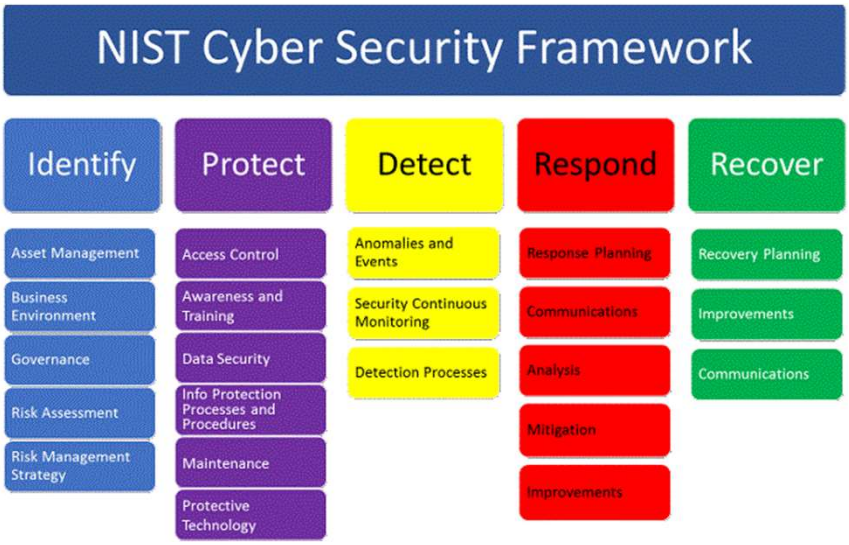
Cyber-Abwehr ist Aufgabe aller Mitarbeitenden

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

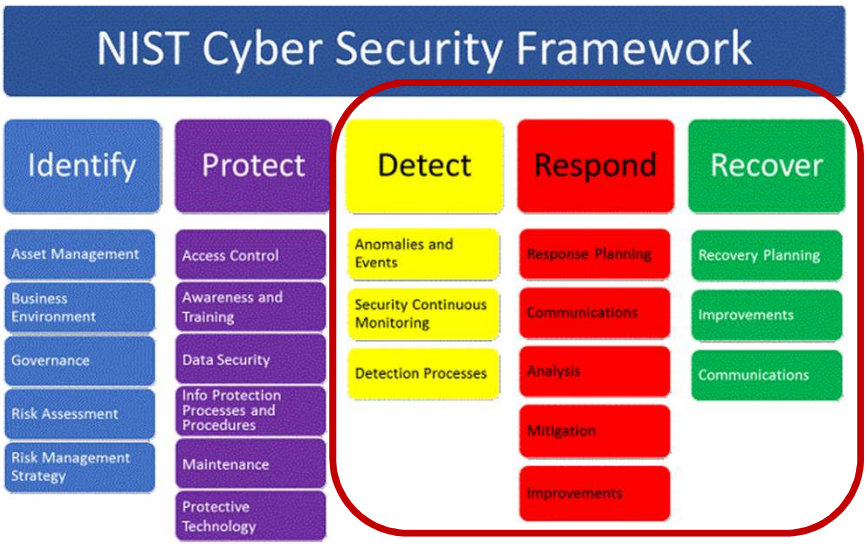
Assume a breach – Vorbereitung ist alles!

AVANTEC
Competence. Security. Trust.



You are under Attack – jetzt schnell reagieren!

AVANTEC
Competence. Security. Trust.

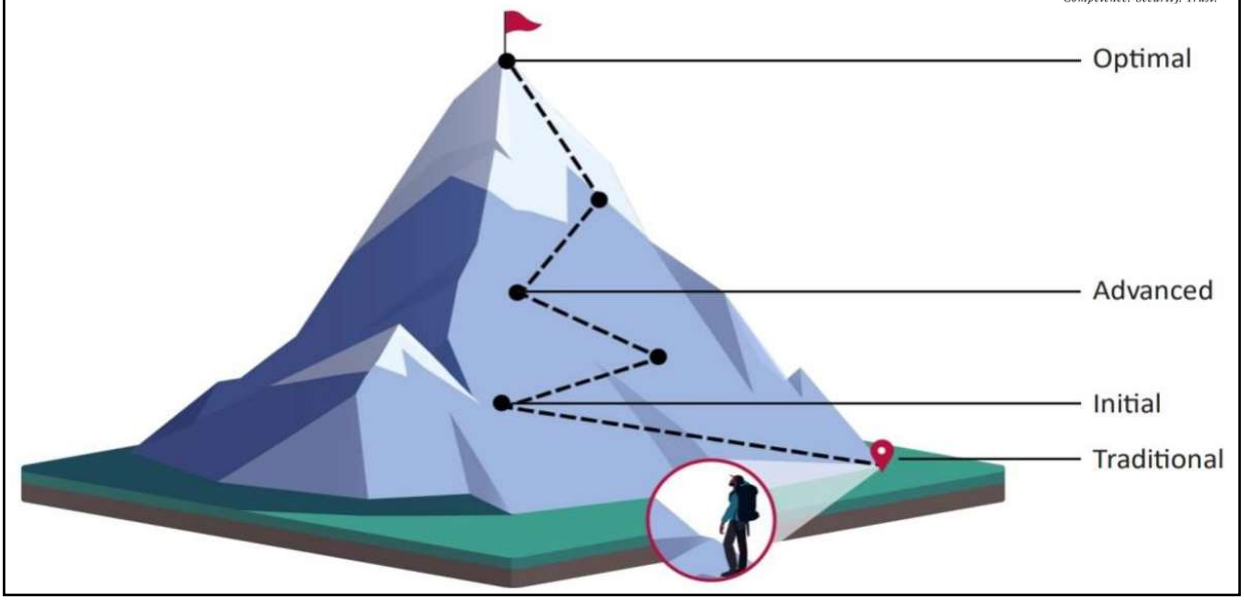


AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Maturität Levels

AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

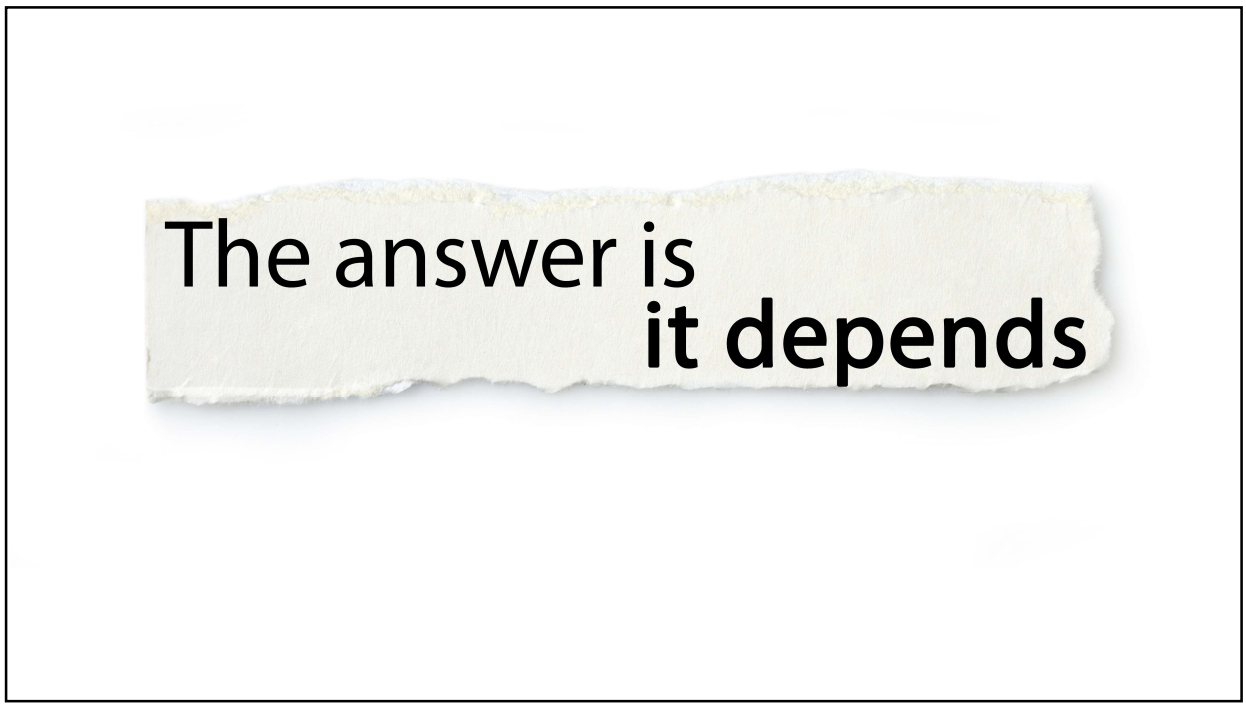
Bei der Cyber-Abwehr geht es um Zeit

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

AVANTEC
Competence. Security. Trust.

Danke



AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Fazit – 7 Schlüsselelemente

1. Discovery – Klassifizierung von Daten und Inventarisierung von Geräten
2. Zentrales Identitäts- und Zugriffsmanagement
   - ❑ Implementieren von IAM, MFA, SSO und PAM
3. Implementieren von Geräte-Sicherheit im IT, IoT und OT Umfeld
   - ❑ Endpoint Security wie Endpoint Detection and Response
   - ❑ Automatisiertes Vulnerability und Patch Management
4. Realisieren von Zero Trust Access zu Applikationen und Workloads (on Premise und Cloud)
   - ❑ Ersetzen von Virtual Private Networks mit ZTNA
5. Implementieren Sie Zero Trust im Netzwerk
   - ❑ Segmentierung (Macro, Micro, Nano) und NAC
   - ❑ Network Detection and Response
   - ❑ DNS Security
6. Verbessern der Visibilität und Analytics
7. Umsetzung von Automatisierung und Orchestrierung

Fazit – 10 Schlüsselelemente

1. Security-Strategie Anpassung: «Der neue Perimeter ist das Device»
2. Security-Strategie Anpassung: «Assume Breach» weg von der Verteidigung, hin zur Detection
3. Definieren Sie Ihre «Zero Trust Maturität»
4. Jede Umgebung ist anders – definieren Sie Ihr «Security Big-Picture»
5. Aktivieren Sie «Multi-Factor-Authentication» für alle Benutzer und Administratoren
6. Ersetzen Sie alle Passwörter – verwenden Sie «Passwordless»
7. Segmentieren Sie Ihr Netzwerk in «Mikrosegmente & Applikations-Zonen»
8. Steuern Sie alle Benutzer, Zugriffe und Geräte über Security Policy Enforcement
9. Verschlüsseln Sie die Daten bei der Übermittlung, bei der Nutzung und im Ruhezustand
10. Führen Sie Zero Trust schrittweise ein, dabei kann die Reihenfolge individuell auf Ihre jetzige Situation angepasst werden

AVANTEC
Competence. Security. Trust.