I'M AFRAID
of what
might happen
if I relax

Ich habe Angst davor, was passieren könnte, wenn ich mich entspanne…

Ausruhen und Security passen nicht zusammen

Christoph Schmidt, Controlware GmbH

#gerneperdu, #staygutdruff, #schmidtinator

16.09.2025, Congress Park Hanau


ZERO
TRUST

Zero Trust

controlware

Was war das nochmal?

Zero Trust basiert auf dem Grundsatz „Never Trust, Always Verify“

Ziel ist es, die Wahrscheinlichkeit und die Auswirkungen von unbefugtem Zugriff zu mindern

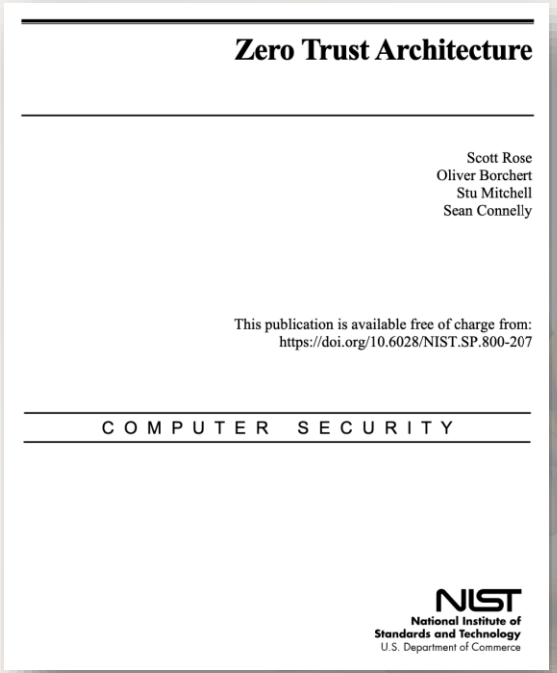
Anforderungen:

- Starke Authentifizierung:
  - Multi-Faktor-Authentifizierung (MFA)
  - Kryptographie
- Netzwerk-Kontrollen:
  - Segmentierung des Netzes
  - Mikro-Segmentierung
- Zugriffskontrollen:
  - Least Privilege
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Attributbasierte Zugriffskontrolle (ABAC)
  - Kontextbasierte Zugriffskontrolle (CBAC)
- Kontinuierliche Überwachung:
  - Kontinuierliche Authentifizierung und Überwachung mit User and Entity Behavior Analytics (UEBA).

Erfordert Überprüfungen, Bewertungen und Audits zur Verstärkung der Sicherheitsmaßnahmen

controlware

Was war das nochmal? NIST



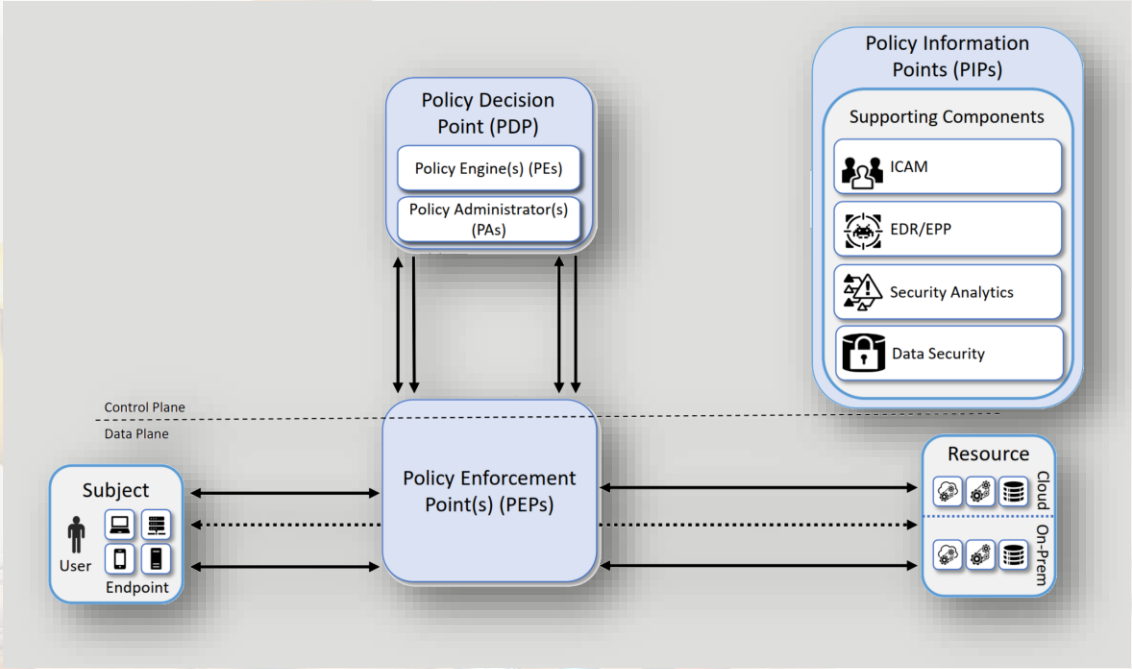
Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

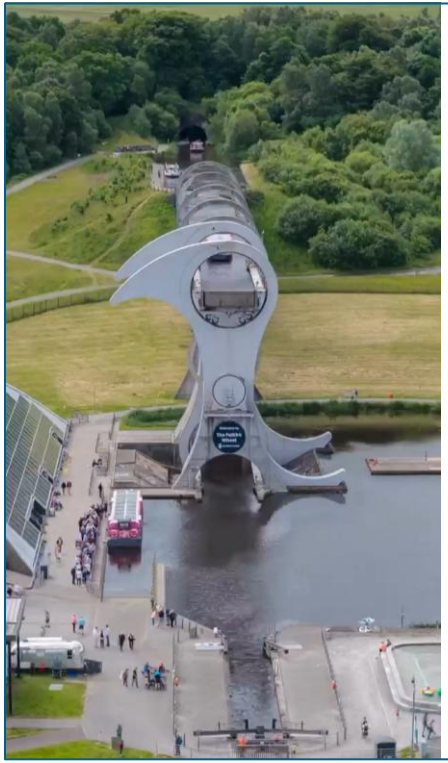
COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



controlware

Segmentierung → feddisch!?



- Identity Segmentation:

- Application Segmentation:

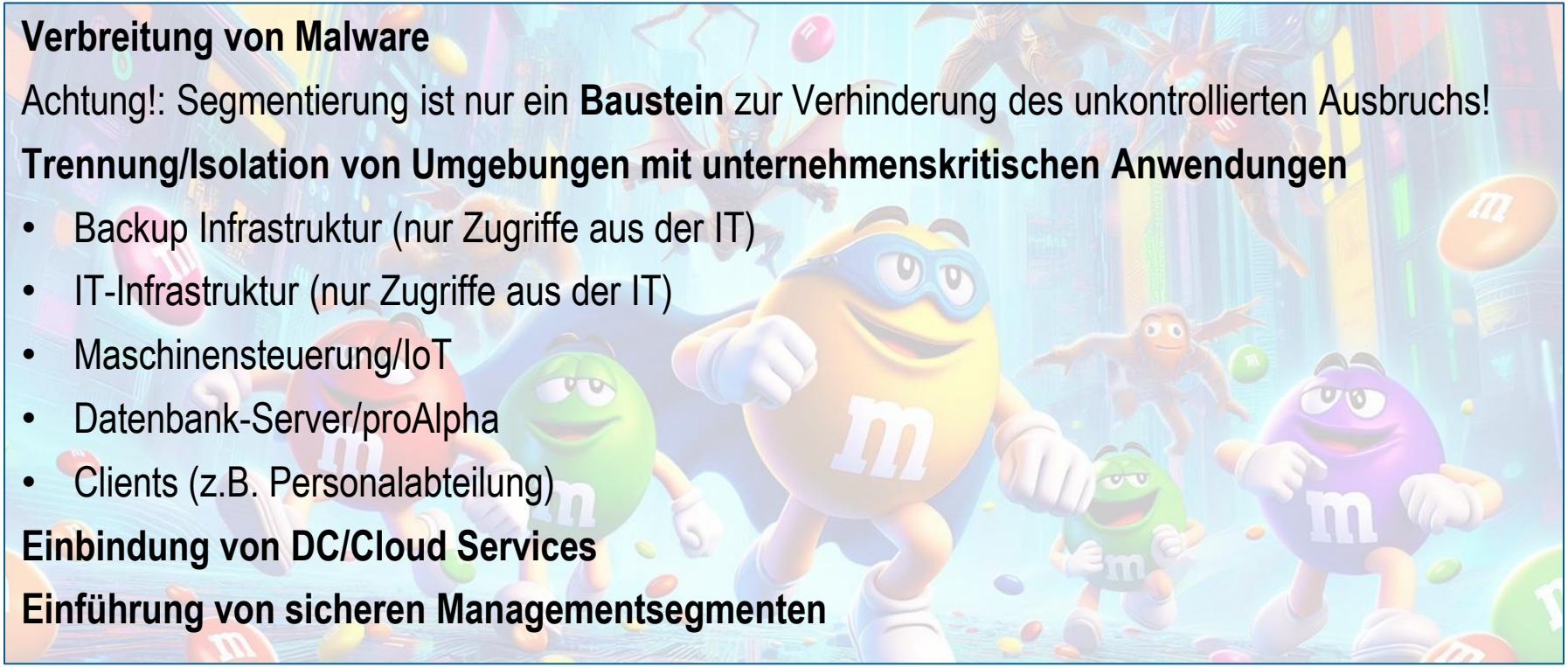
- Device Segmentation:

- Data Segmentation:

Ziele

controlware

Security Redesign



Verbreitung von Malware

Achtung!: Segmentierung ist nur ein **Baustein** zur Verhinderung des unkontrollierten Ausbruchs!

Trennung/Isolation von Umgebungen mit unternehmenskritischen Anwendungen

- Backup Infrastruktur (nur Zugriffe aus der IT)
- IT-Infrastruktur (nur Zugriffe aus der IT)
- Maschinensteuerung/IoT
- Datenbank-Server/proAlpha
- Clients (z.B. Personalabteilung)

Einbindung von DC/Cloud Services

Einführung von sicheren Managementsegmenten

controlware

Segmentierung – Sinn & Zweck

- **Verhinderung unkontrollierter Verbreitung von Malware**
  - Detection & Response (Technisch & Organisatorisch); → eigentlich techn. „Feature“
- **Logische Strukturierung**
- **Schutz von „sensiblen“ Bereichen vor unbefugtem Zugriff**
- **Vereinfachung und Standardisierung der vorhandenen Infrastruktur**
- **Klare Definition zur Bestimmung der Assets und deren Einordnung**


Definitionen

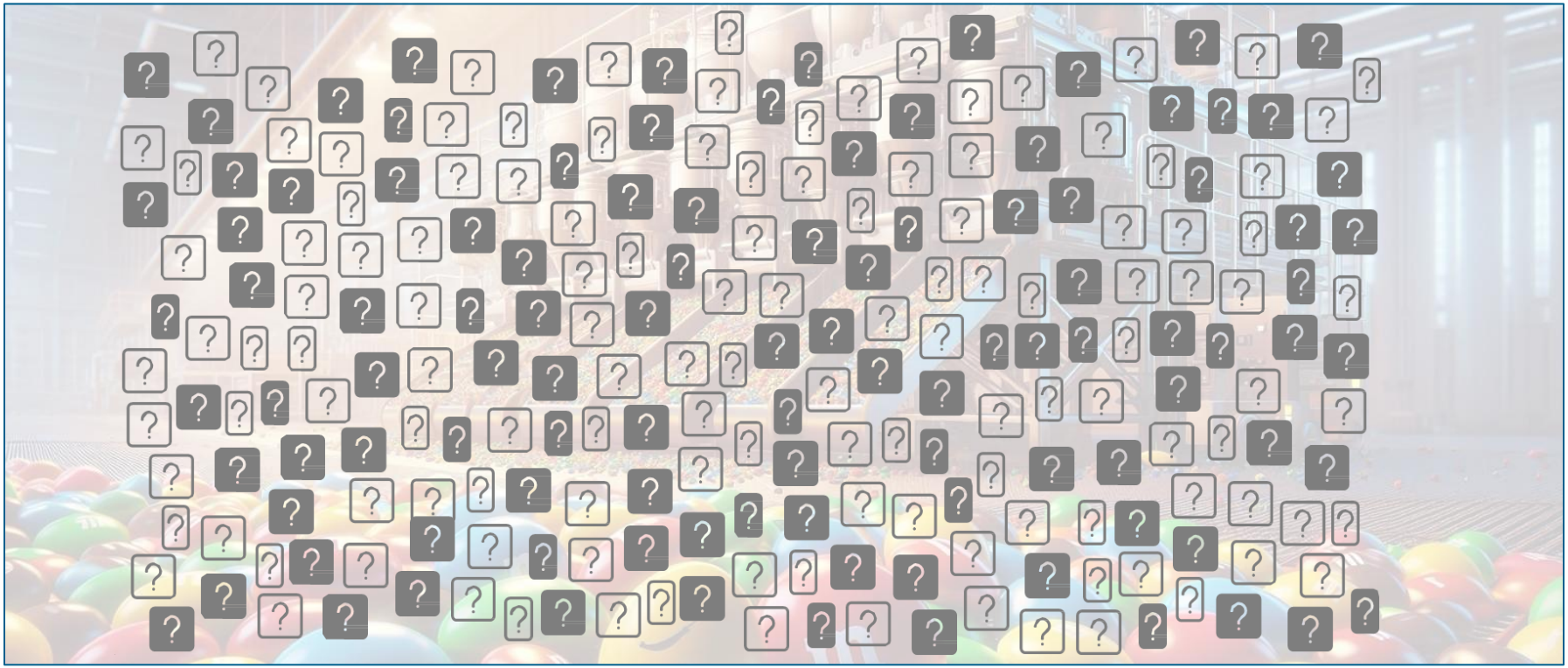
controlware

Kategorisierung der Endsysteme

- **Abbildung der Struktur in jeder Niederlassung!**
- **Kategorisierung aller Endgeräte = Zuordnung in „Containern/Schubladen“**
  - Durch die Kategorisierung erfolgt später die netzwerktechnische Freischaltung des Endgeräts auf Ressourcen (Server, etc.)
  - Vermeidung von Zwittern, d.h. eindeutige Zuordnung von Endgeräten-Schnittstellen

controlware

Kategorisierung der Endsysteme Unbekannt



Definitionen

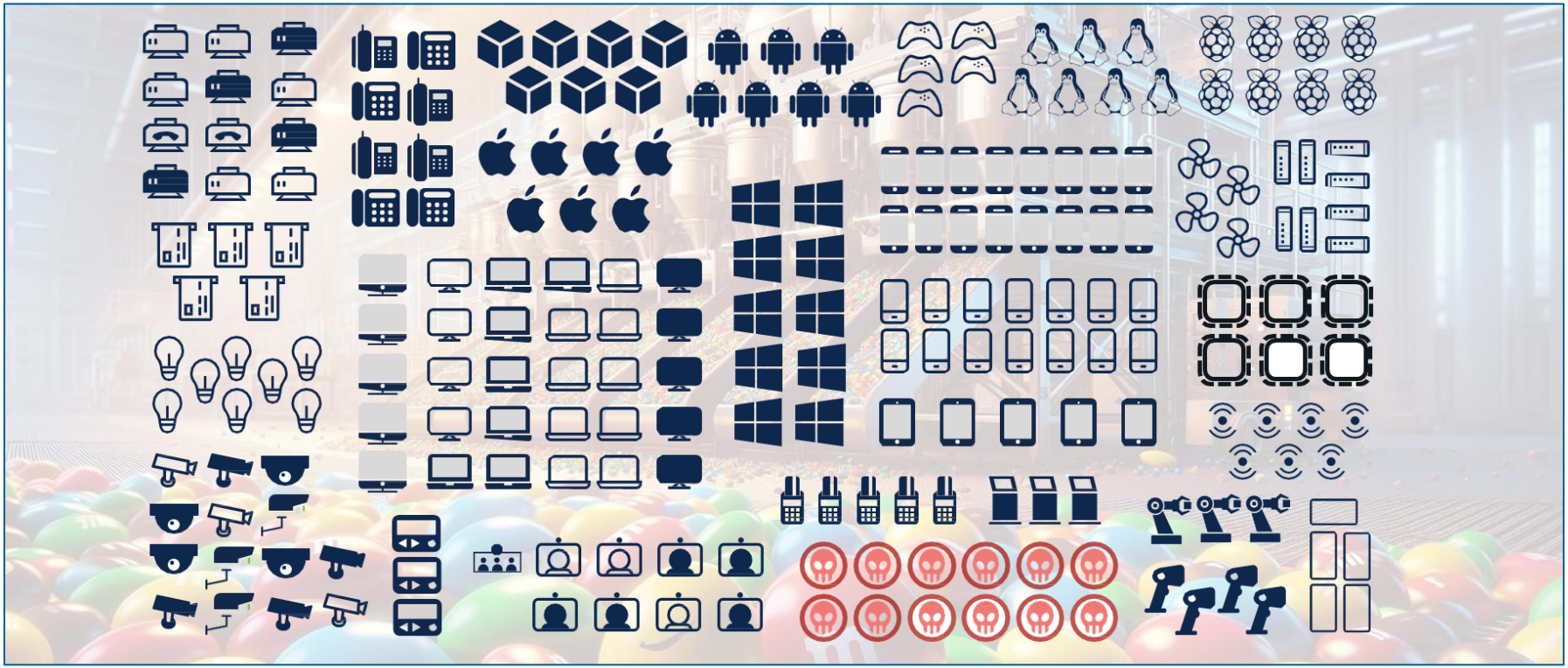
controlware

Kategorisierung der Endsysteme Unbekannt → Bekannt

Definitionen

controlware

Kategorisierung der Endsysteme Unbekannt → Bekannt → Klassifiziert



Definitionen

controlware

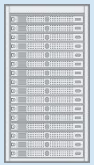
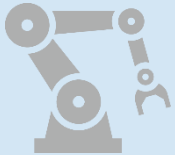
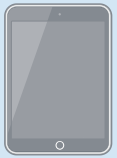
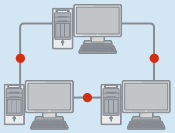
Mensch vs. Maschine

Definitionen

controlware

Kategorisierung der Endsysteme

Endgeräte: Klassifikationen/Kategorien/Schutzzonen/Container

Office	Server	Produktion	Gebäudetechnik	VOICE	Gäste	Management
						
„vollständige“ Arbeitsstationen, Office Rechner, Laptops, Thin Clients Subkategorien • Trusted • Untrusted (keine Überprüfbarkeit von Richtlinienkonformität) • Peripherie (Netzwerkdrucker, MFG)	OnPrem Cloud:XaaS	• Steuerungssysteme • „Workstations“ • Maschinen selbst (IP-fähig)	• Haussteuerungssysteme • IoT • Smart-Systeme (Displays, Projektoren,…)	Tischtelefon Collaboration	Subkategorien • BYOD • Projektmitarbeiter (Fremdfirma) • Wartungstechniker • Temporärer Gast/Zugang • Fremdfirmen permanent (Logistik, Kantinenbetreiber,…)	• Infrastruktur-komponenten (Switches, Router, Firewall,…) • Serveradminis-trationsschnitt-stellen (DRAC, ILO,…) • JumpHost

Definitionen

controlware

Endgeräte – NAC (Network Access Control) – Identifikation & Authentisierung

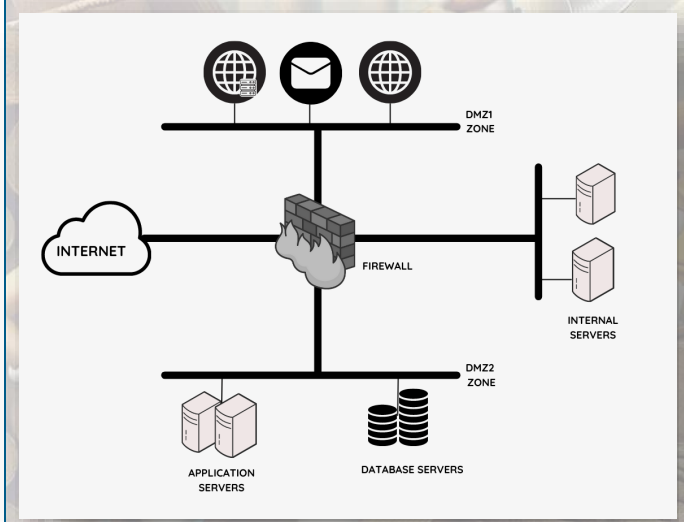
Definitionen

controlware

Endgeräte – NAC (Network Access Control) – „Gesundheitszustand“

controlware

Segmentierung



Network Segmentation, auf Deutsch ***Netzwerksegmentierung***, bezeichnet die Praxis, ein Computernetzwerk in kleinere, isolierte Subnetze oder Segmente zu unterteilen. Ziel ist es, die Sicherheit, Leistung und Verwaltung des Netzwerks zu verbessern. Jedes Segment fungiert dabei als eigenständige Einheit mit spezifischen Zugriffs- und Datenverkehrsrichtlinien.

Definitionen

controlware

Segmentierung – Begriffe

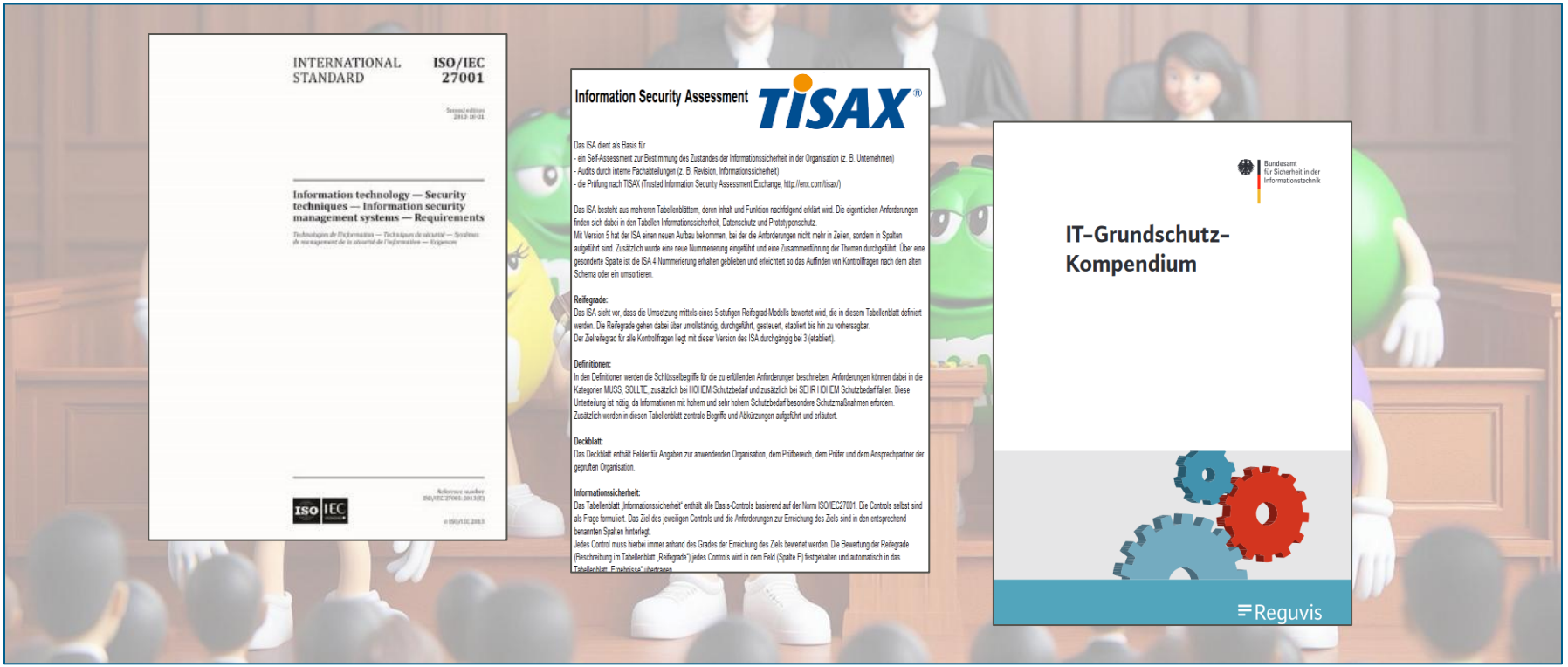
Network Segmentation	Network Compartmentalization	Network Virtualization	Micro Segmentation
• Trennung des Netzwerktraffics in einzelne Bereiche • Hintergrund: „Collision Domains“	• Aufteilen des Netzwerks in Abteilungen oder Zonen (Bsp. Buchhaltung, Personal, F & E, Produktion,…) • Schutzklassen / Schutzzonen	• Logische Trennung von Netzwerken auf einer physikalischen Infrastruktur • VLANs • virtuelle Netzwerkkomponenten • virtuelle Systeme (Hosts, Server, Desktops, usw.)	• Trennung auf Funktionsebene • Im DC: Zugriffe auf Services bzw. Zugriffe von Services untereinander


Das MUSS
so sein...

Rahmenbedingungen

controlware

Regularien



controlware

Regularien – BSI

NET.1.1 Netzarchitektur und –design

- Netztrennung in Zonen
- Client-Server-Segmentierung
- Endgeräte-Segmentierung im internen Netz
- Separierung der Infrastrukturdienste
- Separierung des Management-Bereichs

controlware

Regularien – DORA

Netzwerk Segmentierung Anforderungen unter DORA

Zielsetzung :

- **Verbesserung** der IKT-Sicherheit durch Minimierung des Risikos des unbefugten Zugriffs und Eindämmung potenzieller Verstöße innerhalb isolierter Netzsegmente.

Wichtige Anforderungen :

- Abtrennung und Segmentierung: Umsetzung der Netzabtrennung und -segmentierung auf der Grundlage der Kritikalität, der Klassifizierung und des Risikoprofils von IKT-Systemen und -Netzen.
- Dedizierte Netzwerke: Einrichtung separater und dedizierter Netzwerke für die Verwaltung kritischer IKT-Anlagen, um unbefugten Zugriff zu verhindern.
- Zugangskontrollen: Wenden Sie robuste Netzwerkzugangskontrollen an, um sicherzustellen, dass nur autorisiertes Personal auf sensible oder kritische Netzwerksegmente zugreifen kann..
- Verschlüsselung: Verwenden Sie Verschlüsselung zur Sicherung von Netzwerkverbindungen, insbesondere bei kritischen oder sensiblen Daten, um die Vertraulichkeit und Integrität bei der Übertragung zu gewährleisten..

Umsetzung :

- Mapping und Visualisierung: Effektive Verwaltung und Identifizierung potenzieller Schwachstellen durch Mapping („Kartierung“) und Visualisierung von Netzwerksegmenten.
- Risikobasierter Ansatz: Abtrennung von Netzen durch Bewertung des Risikoprofils und der Kritikalität von Systemen und Daten, um geeignete Sicherheitsmaßnahmen anzuwenden.

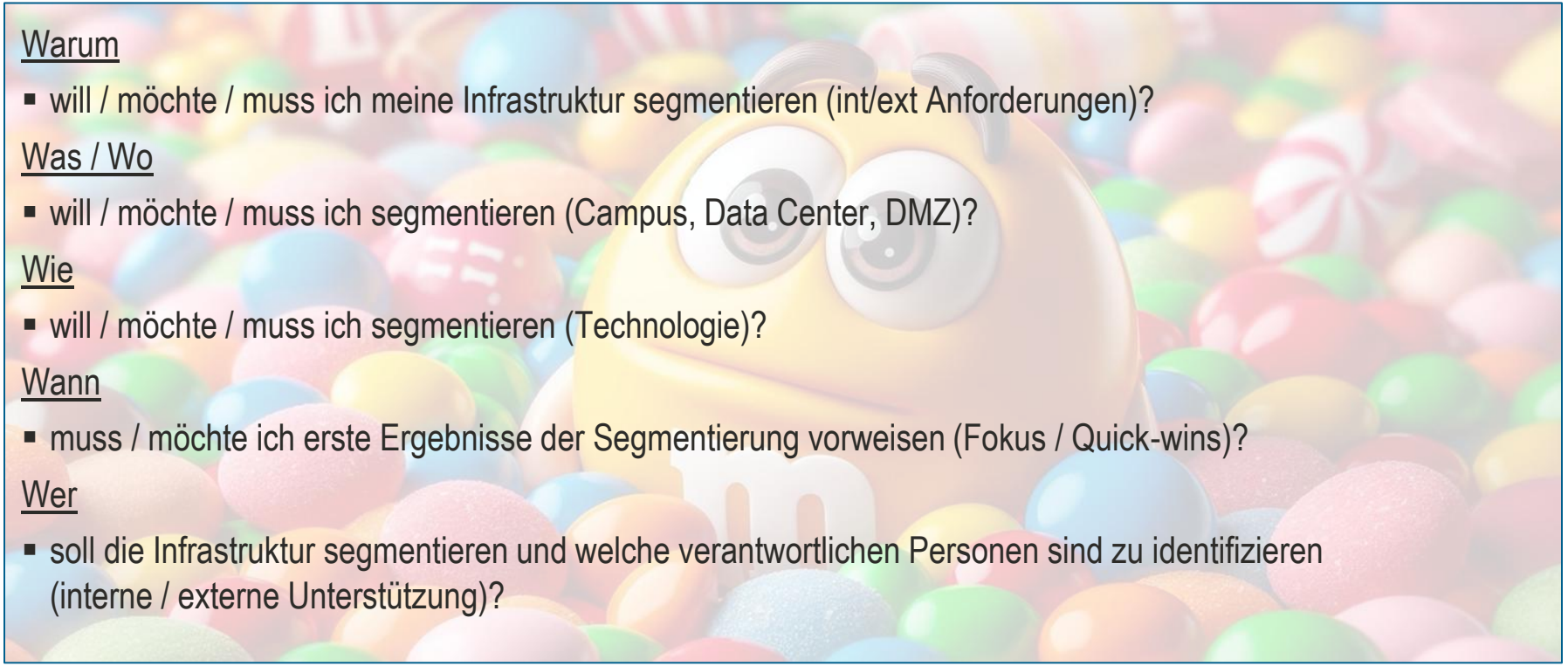
Vorteile :

- Verbesserte Sicherheit: Begrenzung der Verbreitung von Sicherheitsverletzungen und Schutz sensibler Daten.
- Verbesserte Ausfallsicherheit: Isolierung kritischer Systeme zur Gewährleistung eines kontinuierlichen Betriebs bei Sicherheitsvorfällen.

Bevor es jetzt losgeht…

controlware

Die W-Fragen der Segmentierung



Warum

- will / möchte / muss ich meine Infrastruktur segmentieren (int/ext Anforderungen)?

Was / Wo

- will / möchte / muss ich segmentieren (Campus, Data Center, DMZ)?

Wie

- will / möchte / muss ich segmentieren (Technologie)?

Wann

- muss / möchte ich erste Ergebnisse der Segmentierung vorweisen (Fokus / Quick-wins)?

Wer

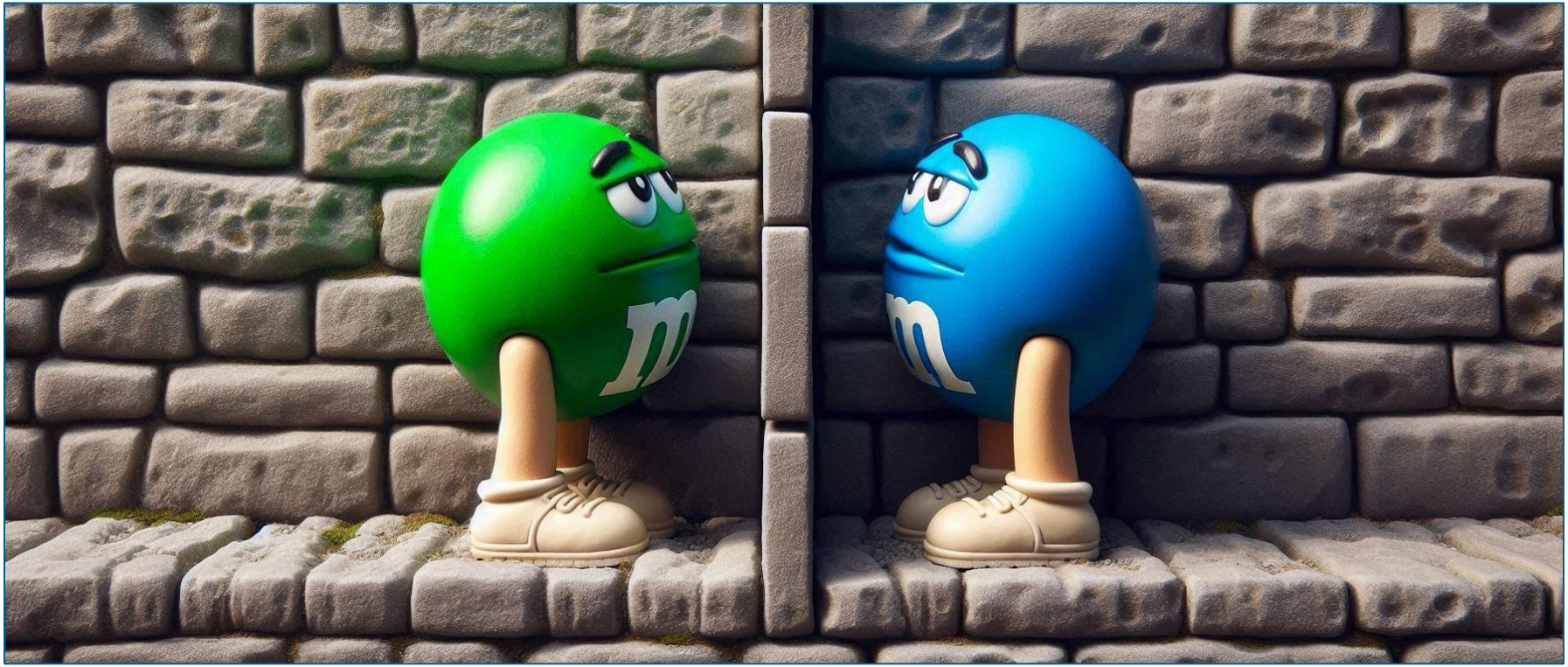
- soll die Infrastruktur segmentieren und welche verantwortlichen Personen sind zu identifizieren (interne / externe Unterstützung)?


Aber wie? Technik

Aufbau von internen Sicherheitszonen / Segmentierung

controlware

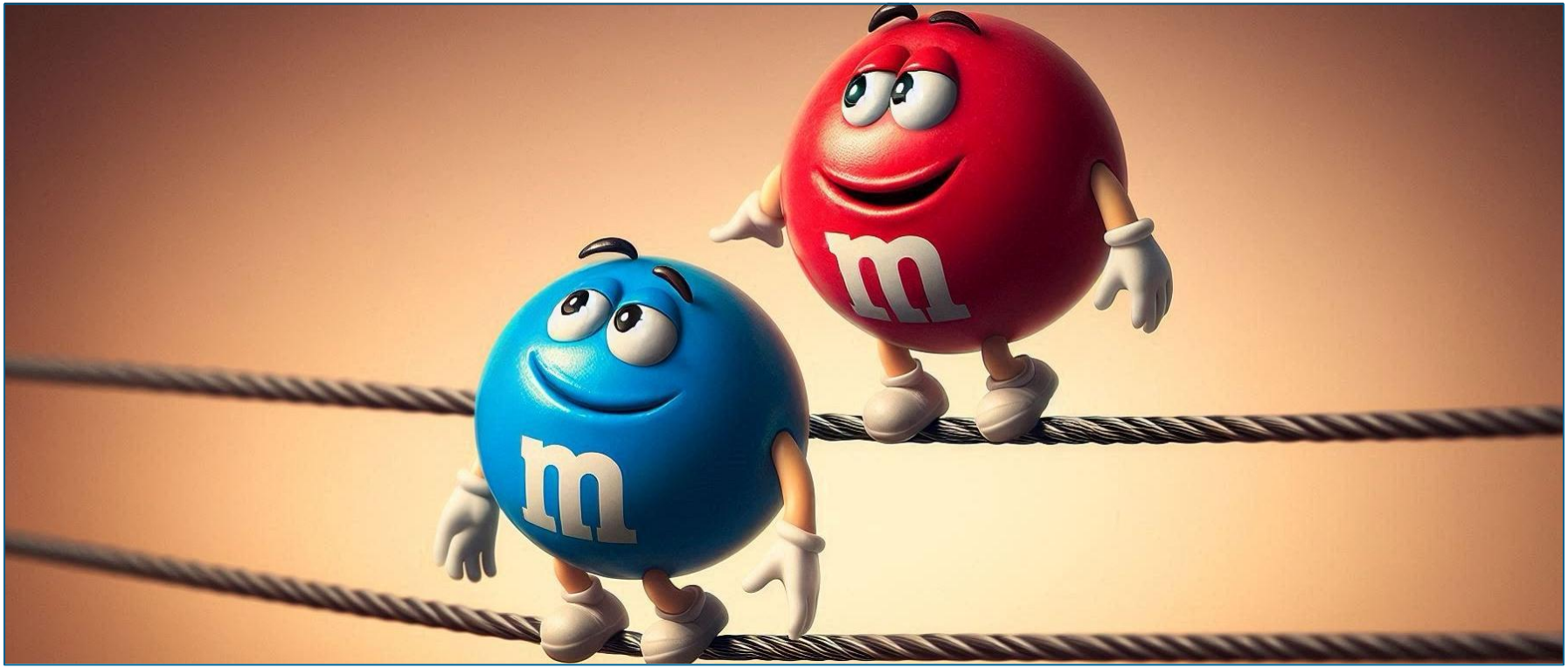
Airgap



Aufbau von internen Sicherheitszonen / Segmentierung

controlware

Physikalisch



Aufbau von internen Sicherheitszonen / Segmentierung

controlware

VLAN

Aufbau von internen Sicherheitszonen / Segmentierung

controlware

Micro-Segmentierung

Aufbau von internen Sicherheitszonen / Segmentierung

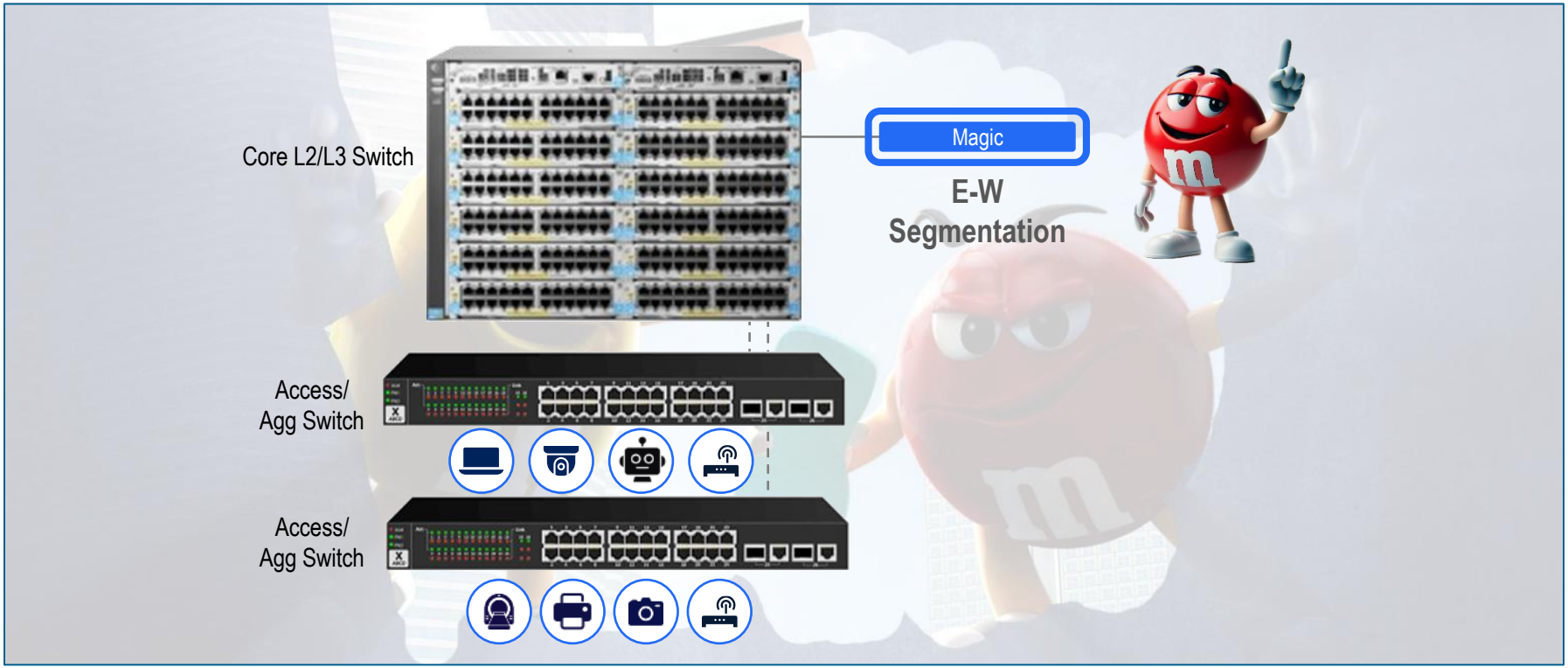
controlware

Geht nicht…

Aufbau von internen Sicherheitszonen / Segmentierung

controlware

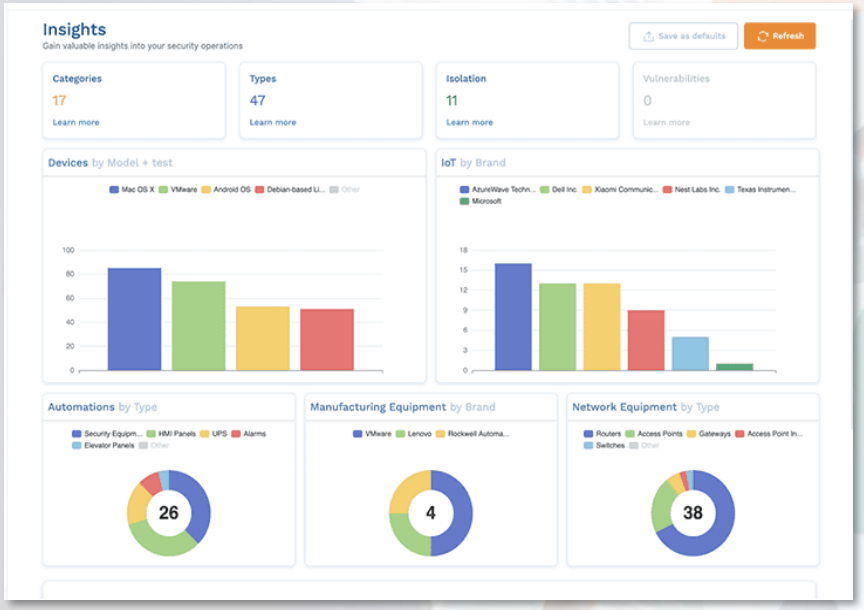
Geht nicht, gibt's nicht!



Aufbau von internen Sicherheitszonen / Segmentierung

controlware

Geht nicht, gibt's nicht!

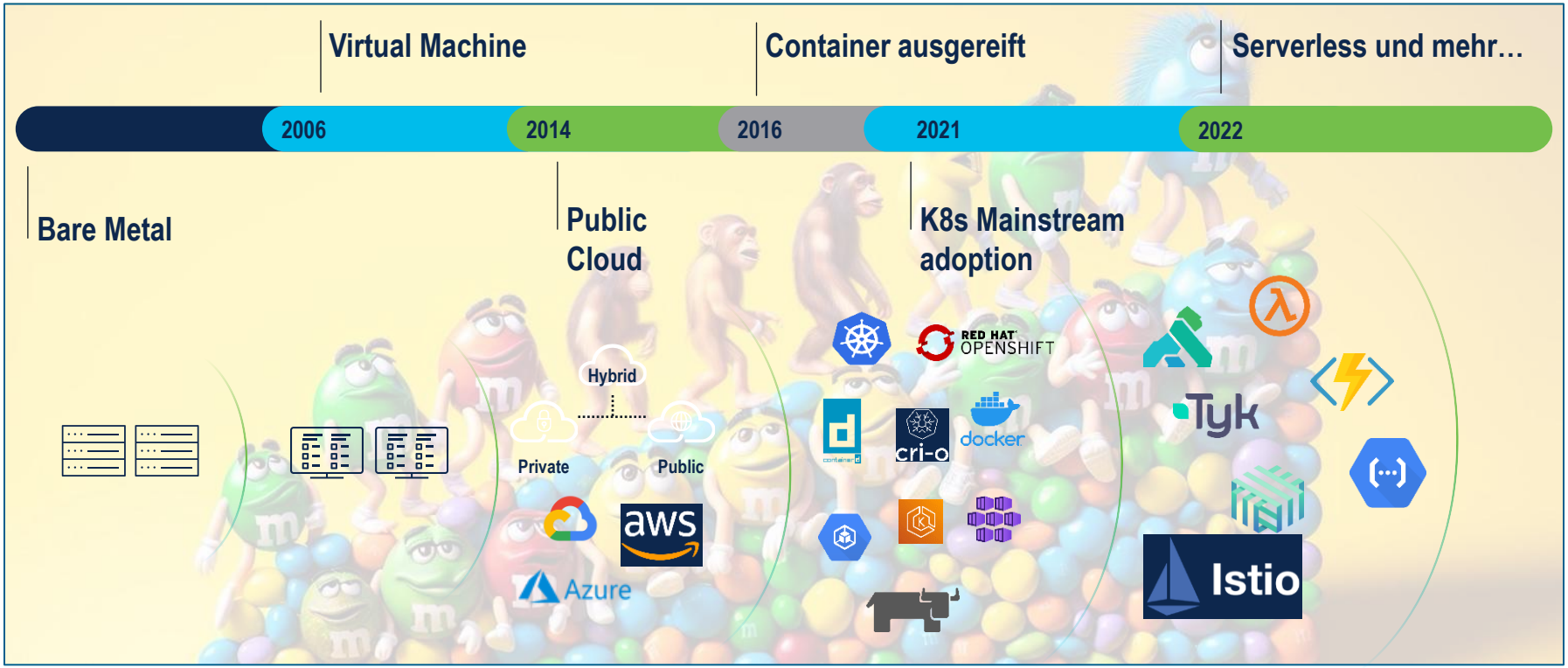



Micro-
Segmentierung

Micro-Segmentierung

controlware

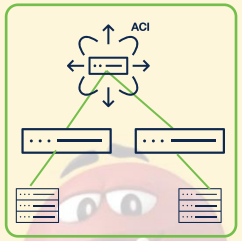
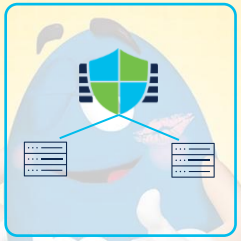
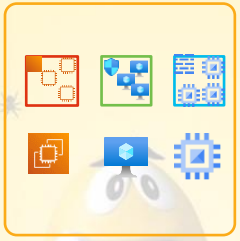
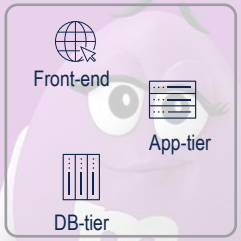
Evolution – Workload



Micro-Segmentierung

controlware

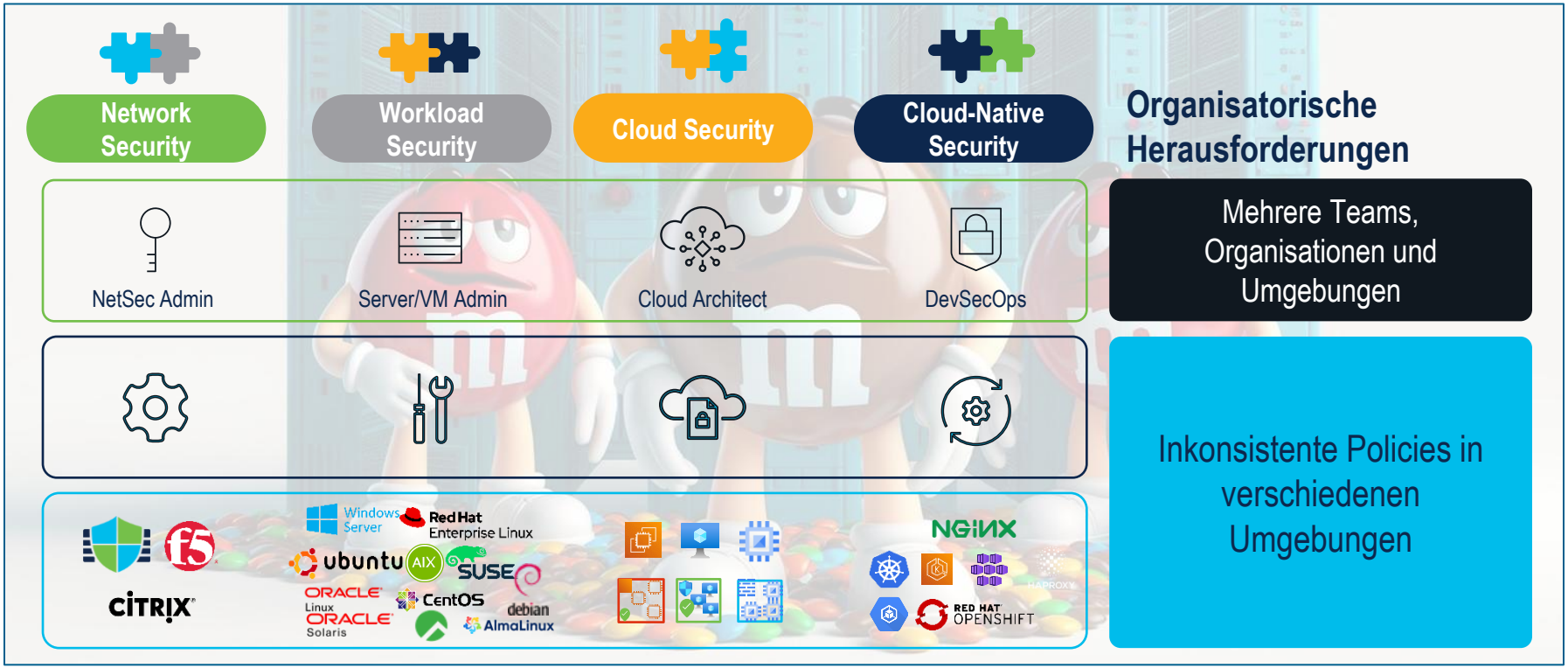
Was ist Application Workload? – Hängt davon ab, wen man fragt

Network Engineer	Firewall Engineer	Cloud Engineer	Application Owners	Cloud-Native Engineer
				
• Vlans/VRF • Subnets • Contracts/PG	• Zones • Subnets • ACLs	• VPC • Subnets • Security Groups	• Service • Application • Workload	• Namespace • Service • CNI

Micro-Segmentierung

controlware

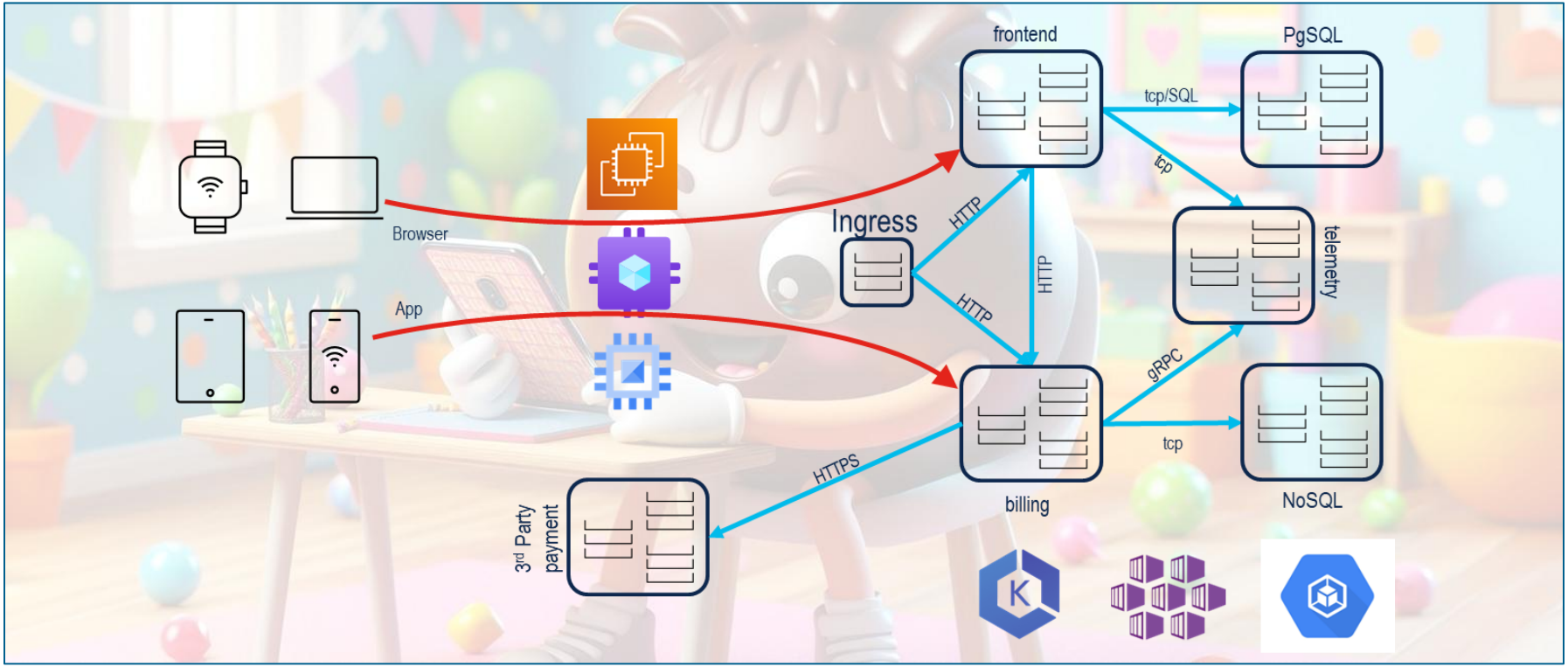
Herausforderungen – Segmentierung & Policy – Zuständigkeit?



Micro-Segmentierung

controlware

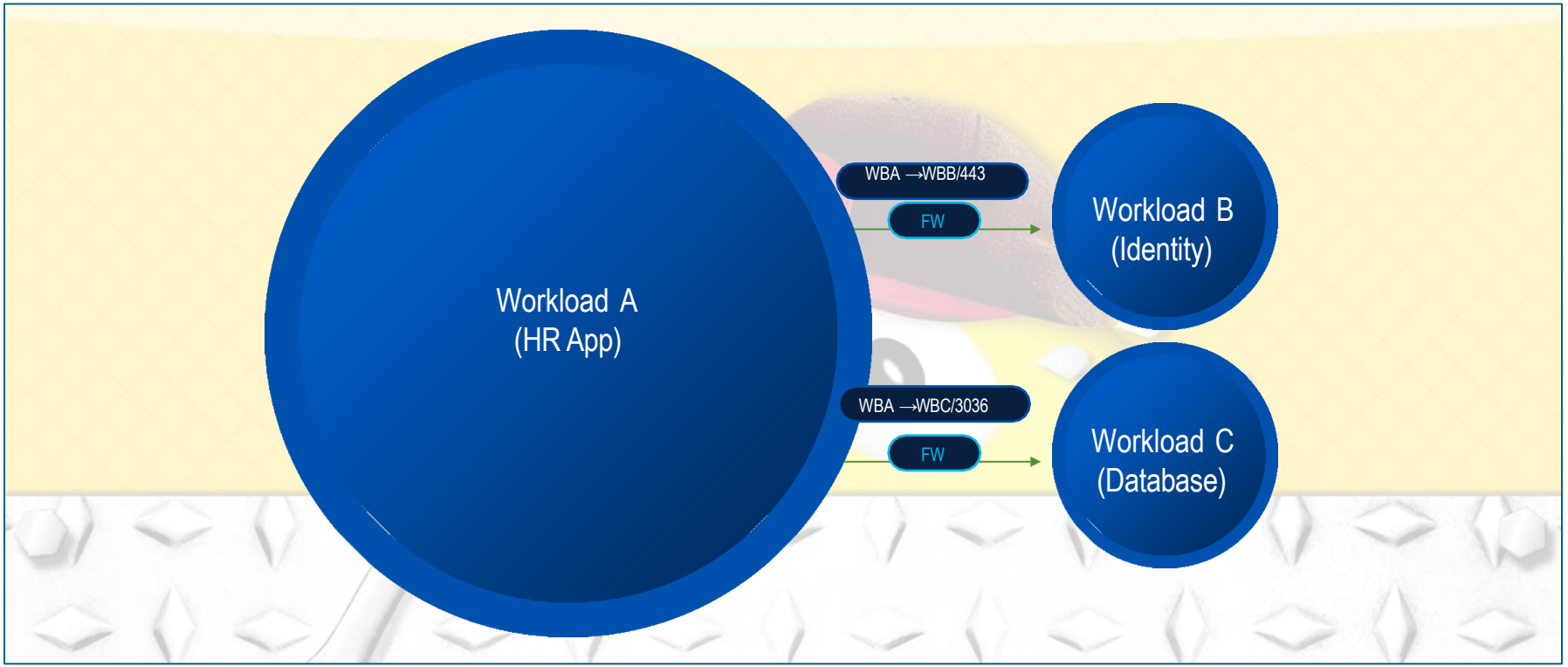
Die Anwendungsarchitekturen haben sich weiterentwickelt



Micro-Segmentierung

controlware

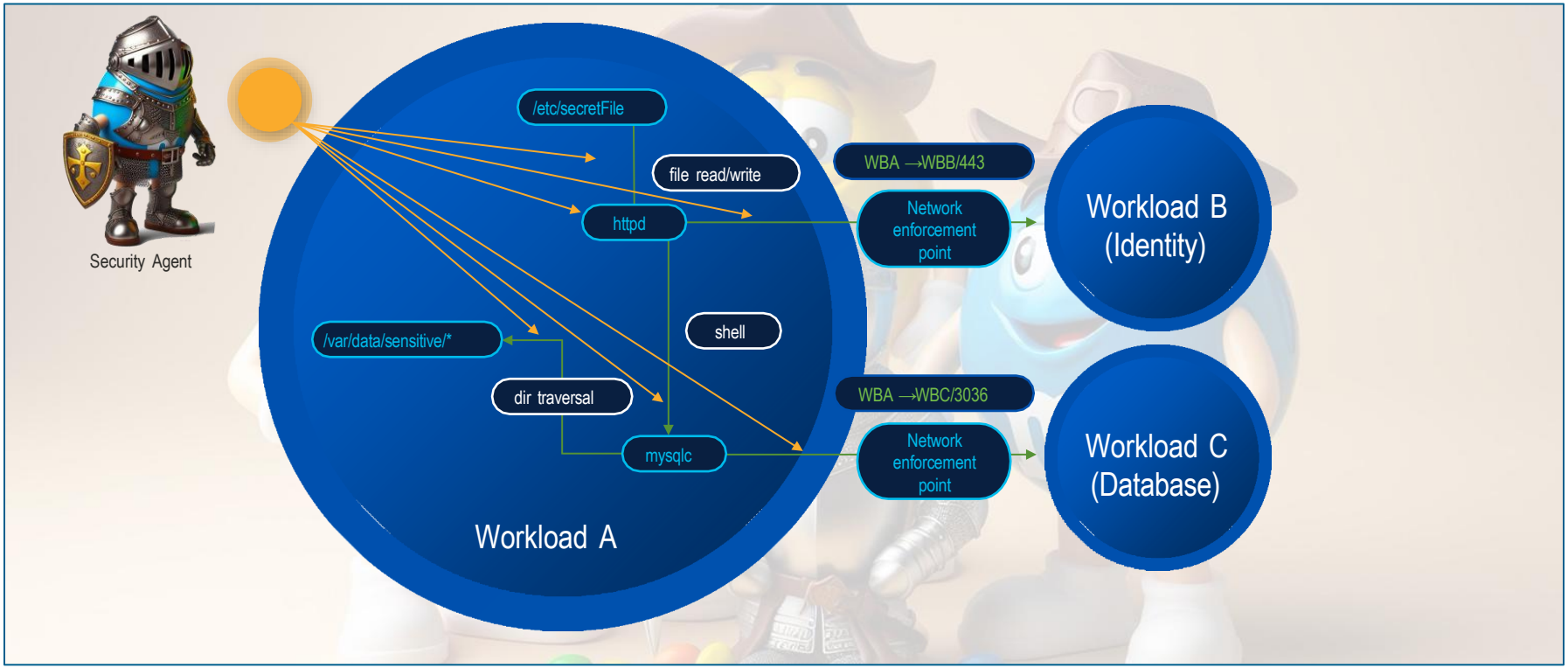
Netzwerk ist limitiert



Micro-Segmentierung

controlware

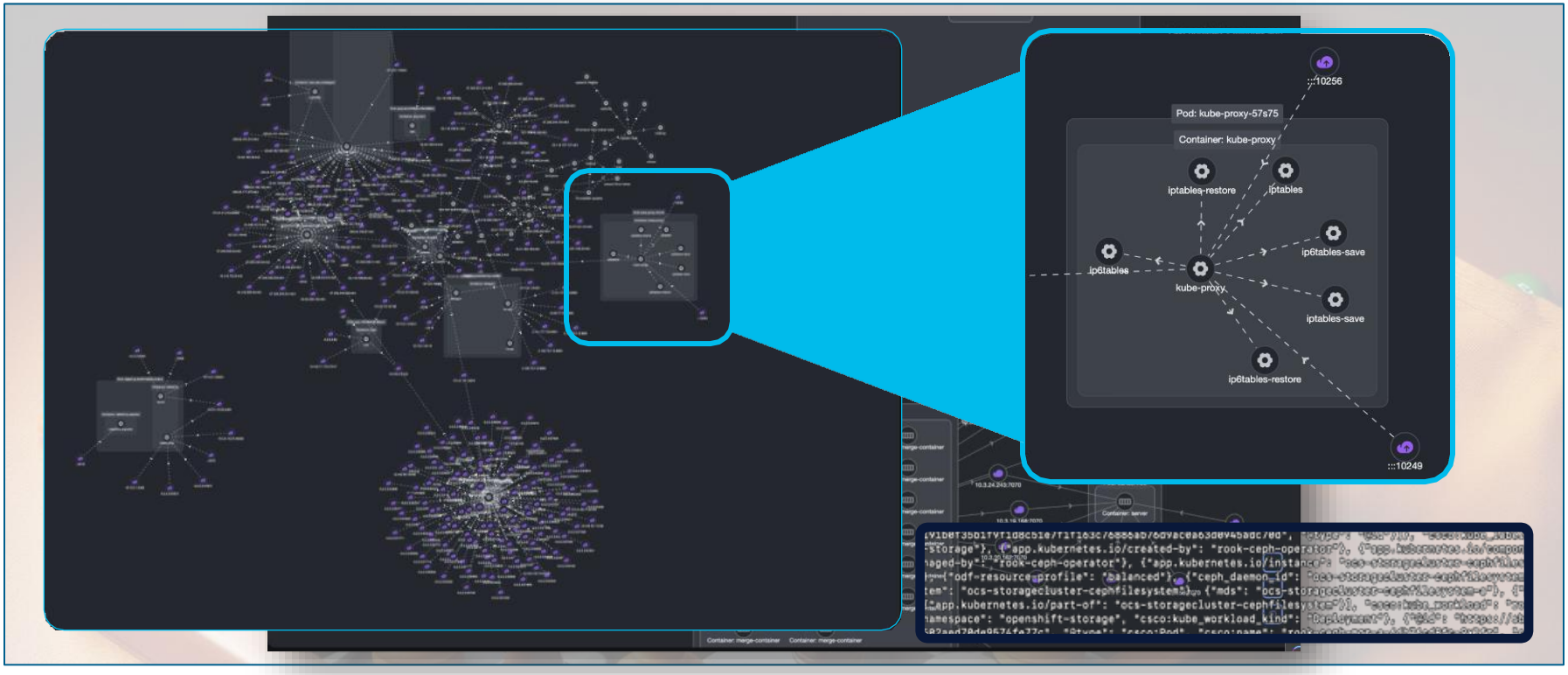
All we need is… More Power…



Micro-Segmentierung

controlware

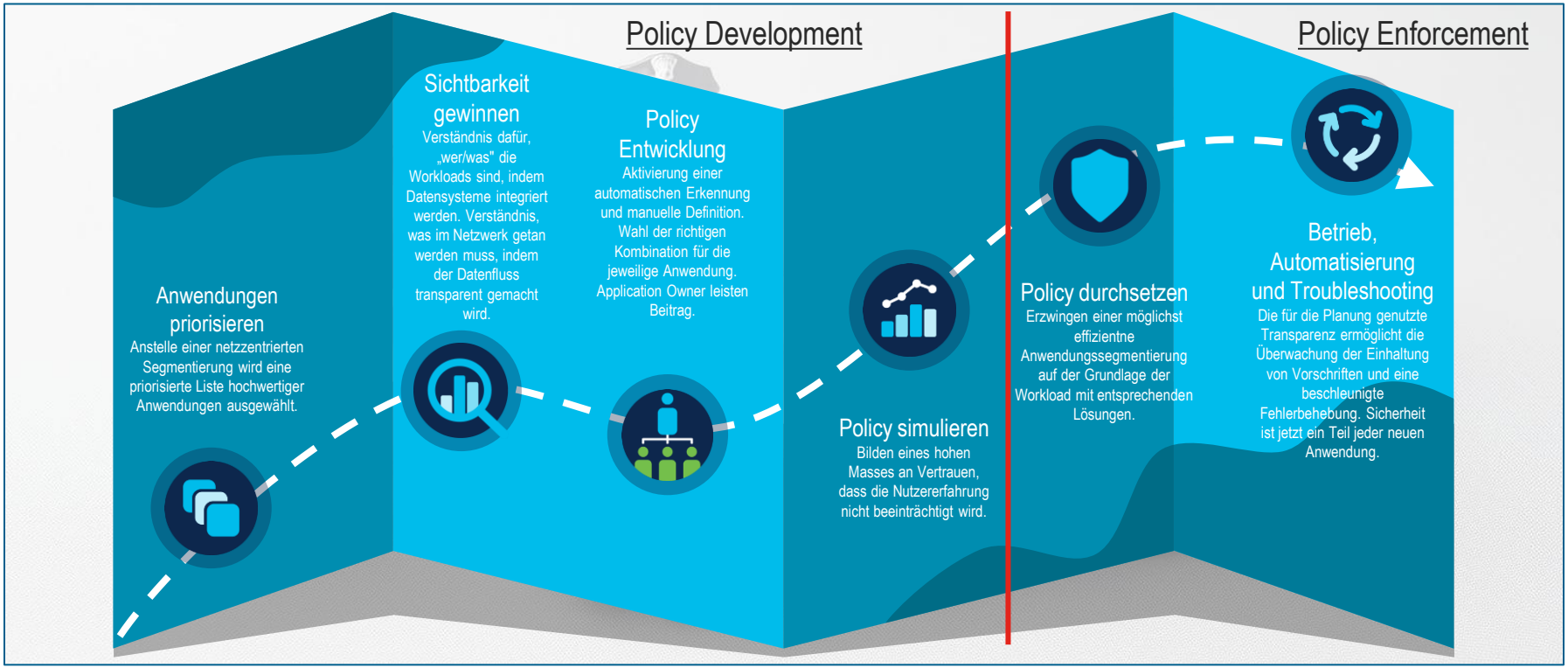
1. Schritt: Sichtbarkeit



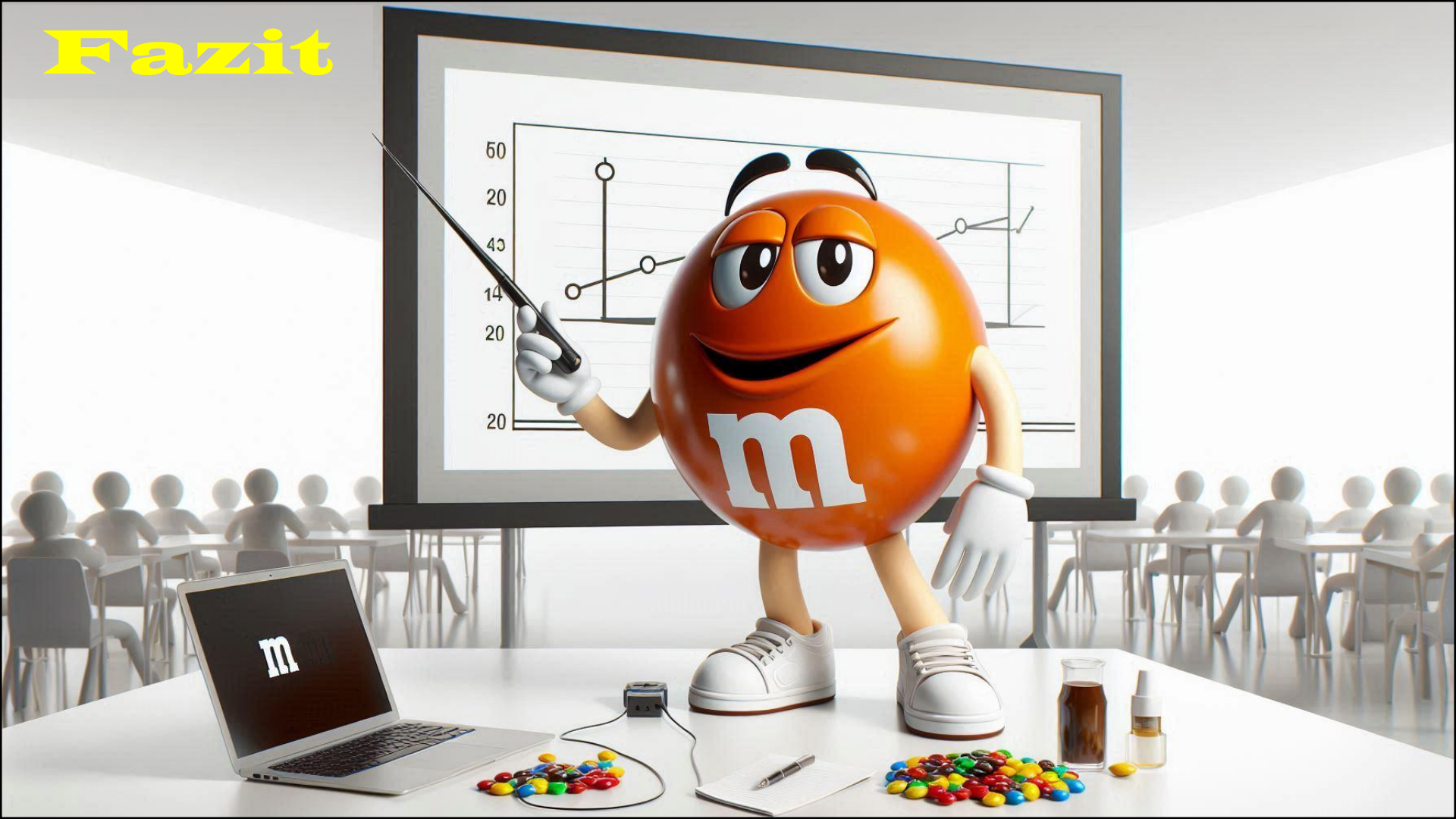
Micro-Segmentierung

controlware

Policy – Vorgehen



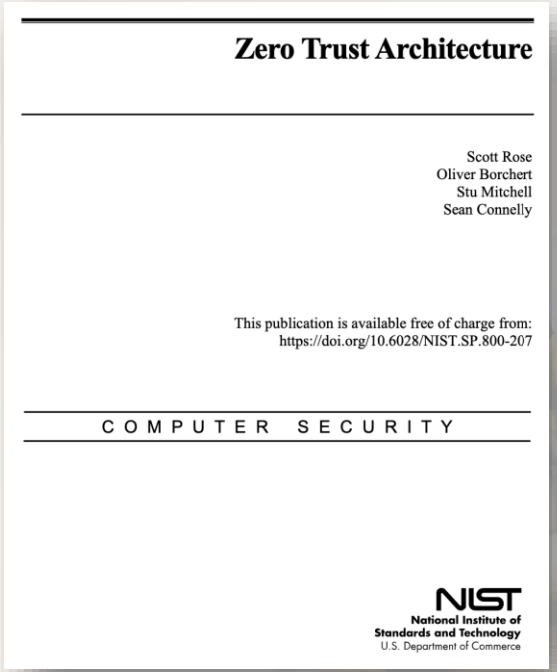
Fazit



Fazit

controlware

Jetzt nochmal mit Zero Trust



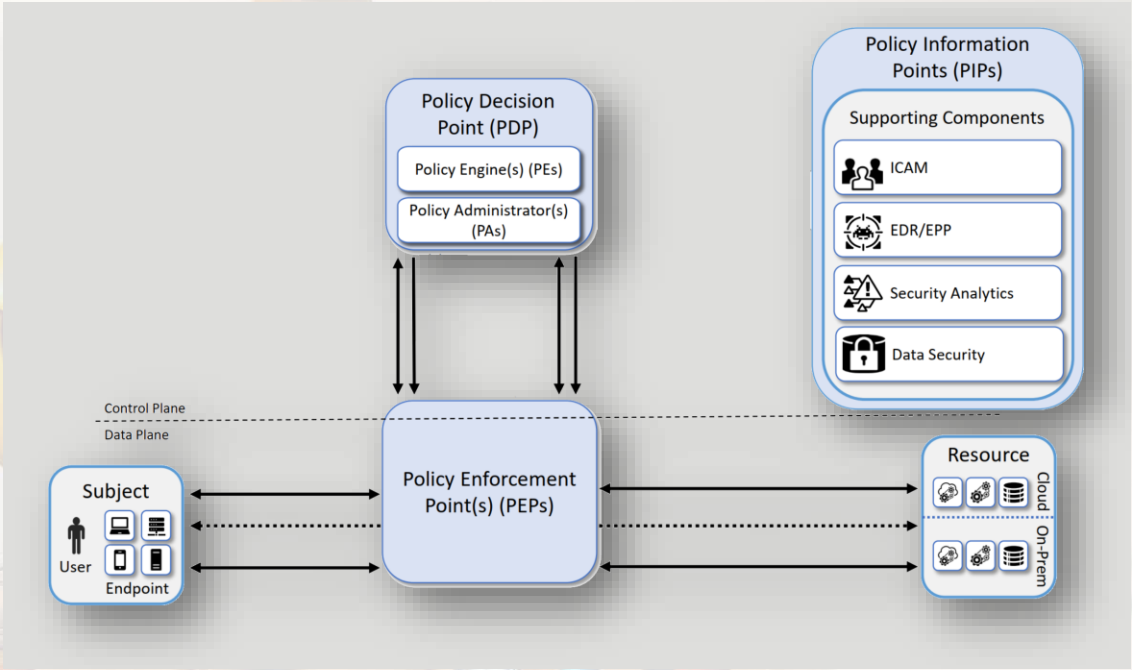
Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

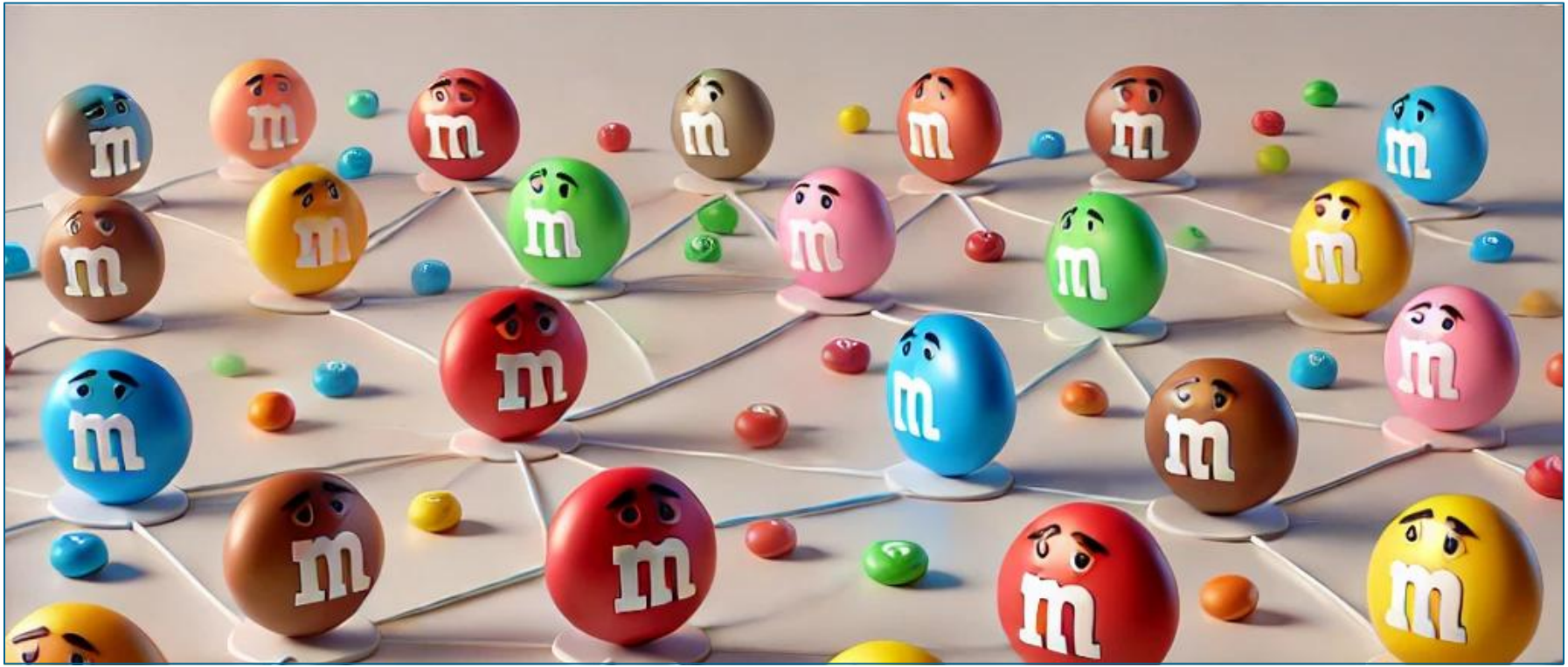
NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Fazit

controlware

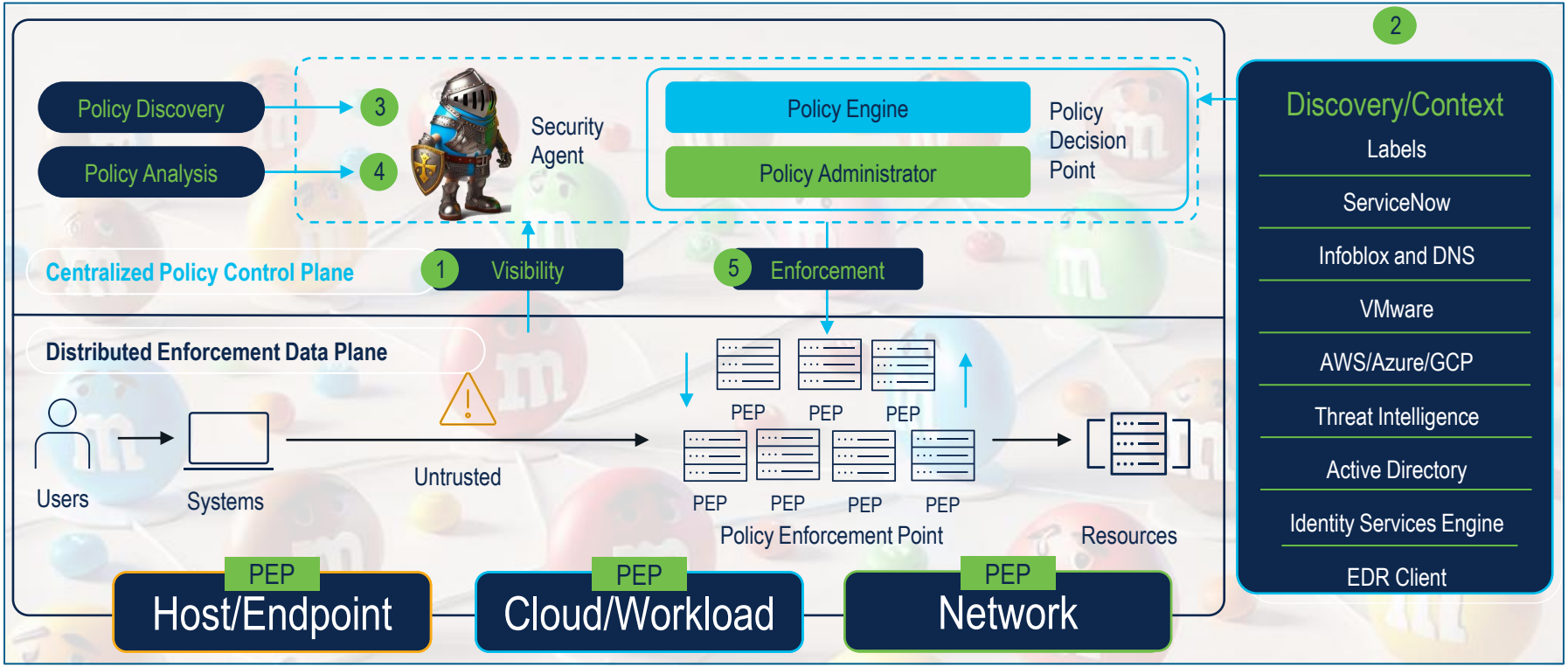
Secure Workload – Zero Trust Segmentation



Fazit

controlware

Secure Workload – Zero Trust Segmentation



controlware

Unn weider? – Vorgehen

Die Netzwerksegmentierung als Prozess und nicht als Projekt angehen.

RISIKO IDENTIFIZIEREN

- Sichtbarkeit gewinnen
- Richtlinien erstellen
- Prioritäten für Veränderungen setzen

DESIGN SEGMENTATION

- Wahl der Methodik
- Zugangskontrolle definieren

BETREIBEN & OPTIMIEREN

- Das Netzwerk überwachen
- Prozesse Iterieren

Information Security

controlware

Strategische Segmentierung (Workshop)

Ungewünschte Bewegungen innerhalb des Netzwerks unterbinden

Situation

Traditionell geplante Netzwerkinfrastrukturen konzentrierten sich in der Vergangenheit eher auf die Konnektivität als auf die Absicherung von Benutzern und der zugrundeliegenden Informationstechnik. Vielfach sorgten dabei u.a. sogenannte Perimeter-Firewalls für den Schutz der internen Netzwerk-Ressourcen. Diese als Perimeter-Modell bekannte Sicherheitsstrategie gilt inzwischen weitgehend als überholt.

Angesichts der zunehmenden Komplexität und Häufigkeit von Cyberangriffen sollten Unternehmen nicht mehr davon ausgehen, dass ihre Sicherheitssysteme und -maßnahmen unüberwindbar sind. Eines der grundlegendsten Probleme ist, dass Angreifer sobald sie einen Zugangspunkt kompromittiert haben, sich relativ leicht innerhalb des Netzes bewegen können. Es existieren praktisch keine Kontrollen, die die so genannten "lateralen Bewegungen" innerhalb des Netzwerks einschränken. Stellen wir uns dazu ein U-Boot ohne wasserdichte Schotten vor. Bei einem Leck würde dieses ohne anderweitige Abwehrmaßnahmen einfach vollaufen und sinken.

Abbildung 1: Schaubild ohne Segmentierung

Herausforderung

Umso komplexer die genutzten IT-Services, desto höher der Sicherheitsaufwand: Die größte Herausforderung ist dabei die fehlende Visibilität im Hinblick auf die Kommunikationsbeziehungen zwischen den Ressourcen. In vergangenen Segmentierungsprojekten hat sich gezeigt, dass die wenigsten Unternehmen ihren Datenverkehr und die Kommunikationsmuster innerhalb des Netzwerkes kennen, verstehen und überwachen.

Eine weitere Herausforderung bei einer traditionellen Segmentierung mittels VLAN und Firewalls ergibt sich bei der VLAN-Migration. Bevor ein Unternehmen die Netzwerksegmentierung implementieren kann, muss es die physikalische oder logische Aufteilung der Geräte in verschiedene Segmente durchführen. Die VLAN-Migration erfordert eine sorgfältige Planung und Ausführung, da eine fehlerhafte Umsetzung zu Ausfällen oder Konnektivitätsproblemen führen kann. Ferner ist es wichtig, dass die gewählte VLAN-Struktur ausreichend Flexibilität für sich ändernde Anforderungen bietet.

Die Erstellung und Verwaltung von Regelwerken für die einzelnen Segmente ist ebenfalls sehr zeitaufwändig. Die Sicherheitsrichtlinien müssen so gestaltet werden, dass sie die spezifischen Anforderungen jeder Sicherheitszone erfüllen und gleichzeitig das reibungslose Funktionieren der Geschäftsprozesse ermöglichen. Die fein abgestimmten Regelwerke müssen regelmäßig aktualisiert werden, um sicherzustellen, dass sie immer noch angemessen und wirksam sind.

Trotz dieser Aufwände ist die Isolierung und Segmentierung von Anwendungen und ihren Komponenten im Netzwerk notwendig, um mögliche Compliance-Vorgaben einzuhalten und Unternehmensanwendungen und -daten gegen Cyberattacken zu schützen. Unser U-Boot behält durch eine wasserdichte Segmentierung, im Fall eines Lecks, seine Schwimmfähigkeit.

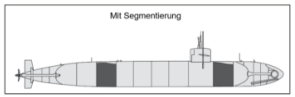


Abbildung 2: Schaubild mit Segmentierung

Lösungsansätze

Historisch gewachsene flache Netzwerke müssen umgebaut, modernisiert und umstrukturiert werden, damit sie den Sicherheitsanforderungen von heute und morgen gerecht werden.

Eine Kombination aus Makro- und Mikrosegmentierung hat sich als eine fortschrittliche Netzwerksegmentierungsstrategie etabliert. Diese bietet sowohl eine grobe

General Topic

controlware

Zero Trust – Übersicht

Workshop zur Standortbestimmung für geplante bzw. begonnene Zero Trust Initiativen

Die Situation
Traditionelle IT-Infrastrukturen benötigen ein Redesign zur Unterstützung der Digitalen Transformation

Zero Trust ist ein Sicherheitskonzept, das darauf abzielt, die Netzwerksicherheit zu verbessern, indem grundsätzlich keinem Benutzer, Gerät oder Netzwerkverkehr blind vertraut wird, selbst wenn sie sich innerhalb des Netzwerks befinden. Traditionell wurde in Netzwerken oft ein "Perimeter-basiertes" Sicherheitsmodell verwendet, bei dem das interne Netzwerk als vertrauenswürdig angesehen wurde und der Zugriff auf Ressourcen innerhalb des Netzwerks relativ offen war.

Zero Trust basiert auf der Annahme, dass keine Entität innerhalb oder außerhalb des Netzwerks automatisch vertrauenswürdig ist. Stattdessen erfordert es eine kontinuierliche Überprüfung und Überwachung der Identität, des Zustands und des Verhaltens von Benutzern, Geräten und Netzwerkverkehr.

Durch die Implementierung von Zero Trust werden Sicherheitsmaßnahmen wie mehrstufige Authentifizierung, Zugriffskontrollen, Verschlüsselung, Anomalieerkennung und Überwachung angewendet.Das Prinzip „Least Privilege“, bei dem Benutzer nur Zugriff auf die Ressourcen erhalten, die sie für ihre Arbeit benötigen, ist elementarer Bestandteil von Zero Trust.

Zero Trust bietet mehrere Vorteile, darunter:

- Erhöhte Sicherheit: Durch die kontinuierliche Überprüfung und Verifizierung von Benutzern und Geräten wird das Risiko von Kompromittierung und Datenverlust reduziert.
- Bessere Sichtbarkeit: Zero Trust ermöglicht eine detaillierte Überwachung der Kommunikation, sodass verdächtige Aktivitäten schneller erkannt werden können.
- Schutz vor internen Bedrohungen: Da Zero Trust keinen blinden Vertrauensvorschuss gewährt, werden auch interne Benutzer und Geräte überwacht, um böswillige Aktivitäten zu erkennen.
- Flexibilität: Zero Trust ermöglicht es Organisationen, verschiedene Arten von Benutzern (Mitarbeiter, Auftragnehmer, Partner usw.) und Geräten (BYOD, IoT usw.) sicher in ihr Netzwerk einzubinden.

Es ist jedoch wichtig zu beachten, dass Zero Trust kein (einzelnes) Produkt oder Technologie ist, sondern ein umfassendes Sicherheitskonzept, das eine Kombination verschiedener Maßnahmen erfordert.

Die Herausforderung
veränderte Bedrohungslandschaft, veränderte Arbeitsweisen

Die aktuelle Situation rechtfertigt die Implementierung einer Zero Trust-Architektur aus mehreren Gründen:

Veränderte Bedrohungslandschaft: Eine Zero Trust-Architektur bietet zusätzliche Schutzmechanismen, um Angriffe wie Phishing, Ransomware, Advanced Persistent Threats (APTs) und Insider-Bedrohungen zu erkennen und abzuwehren.

Dezentralisierung der Netzwerke: Zero Trust ermöglicht eine granulare Kontrolle über den Netzwerkzugriff, unabhängig vom Standort oder Gerät.


Controlware
Security Day
controlware
Vielen Dank für Ihre Aufmerksamkeit!
Controlware Security Day 2025