Zero Trust Foundation

Januar 2025 | Simon Taylor

q.beyond

Zero-Trust als Grundlage für sicheres Arbeiten

Die globale Pandemie hat den bereits laufenden grundlegenden Wandel im Sicherheitsbereich beschleunigt und zahlreiche Herausforderungen hervorgehoben. Traditionelle, perimeterbasierte Netzwerk- und Sicherheitsmodelle konnten sich nicht ausreichend anpassen und viele Infrastrukturen waren auf den massiven Übergang zur Remote-Arbeit nicht vorbereitet. Unser Dienstleistungsangebot umfasst die folgenden Leistungen:

- **Entwicklung eines Bereitstellungsplan für Zero Trust, der die Schritte zur Implementierung von Zero Trust mit Microsoft 365 in Ihrer Organisation skizziert**
- **Konfiguration von Zero Trust Identitäts- und Gerätezugriffsschutz durch die Einrichtung von Basisrichtlinien und die Verwaltung von Endpunkten mit Intune**
- **Erweiterung der in Microsoft 365 integrierten Sicherheits- und Informationsschutzfunktionen auf alle an Entry ID angebundenen SaaS-Apps, um die Zugriffe zentral zu verwalten und die Daten in den Apps zu schützen**
- **Bedrohungsschutz durch KI-gestützte Überwachung der Umgebung, Darstellung aktueller Risiken und automatisierte Maßnahmen zur Abwehr von Angriffen**
- **Unterstützung bei der Implementierung und Verwaltung von Zero Trust in Ihrer Organisation sowie Schulung Ihrer Mitarbeiter zur Nutzung und zum Verständnis von Zero Trust**
- **Regelmäßige Überprüfung und Anpassung der Zero Trust-Strategie, um auf sich ändernde Bedrohungen und Geschäftsanforderungen zu reagieren**

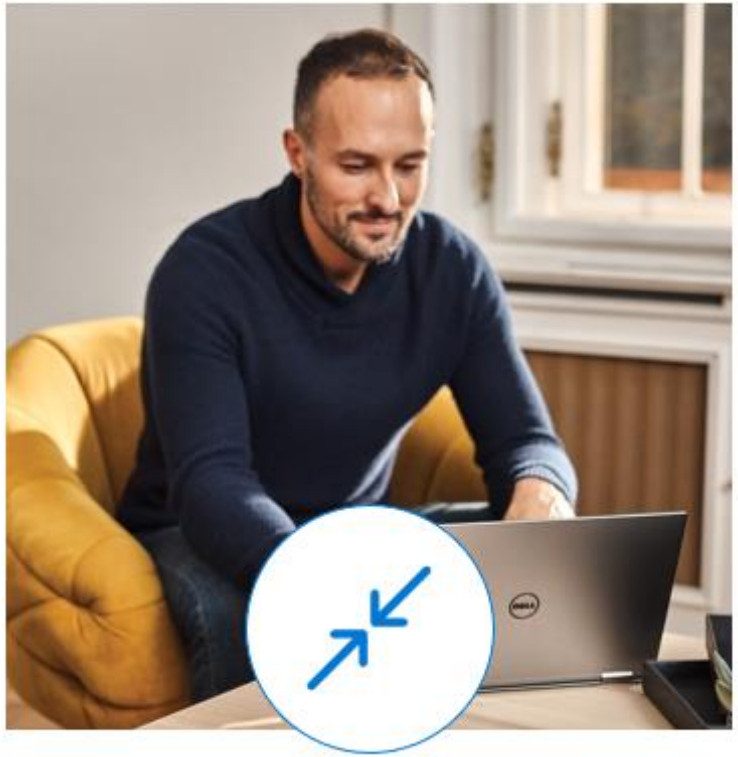
Mit unserem Dienstleistungsangebot für die Schaffung der Grundlagen von Zero-Trust helfen wir Ihnen, die Anforderungen and einen grundlegenden modernen Identitäts- und Zugriffsschutz zu erfüllen und damit die Betriebssicherheit Ihres Unternehmens nachhaltig zu sichern. Wir sind überzeugt, dass Sie mit einem modernen Arbeitsplatz die Produktivität, Innovation und Zufriedenheit in Ihrem Unternehmen steigern und sich einen Wettbewerbsvorteil verschaffen können.

Bausteine der Zero-Trust Strategie

q.beyond

Zero-Trust-Prinzipien

Zugriffe immer explizit überprüfen

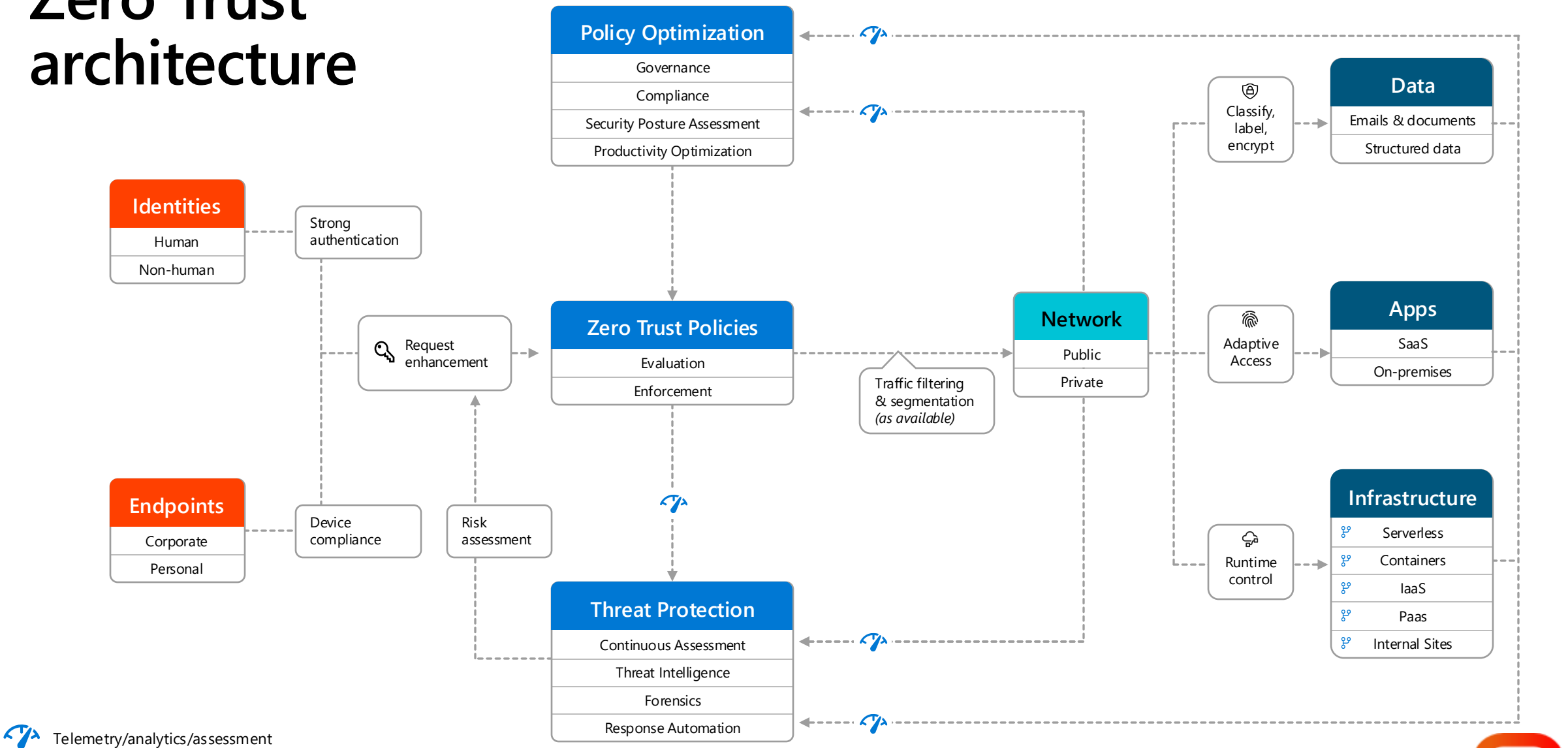


Zugriff mit den geringsten Berechtigungen

Annahme des Datenverlustes

Zero Trust architecture

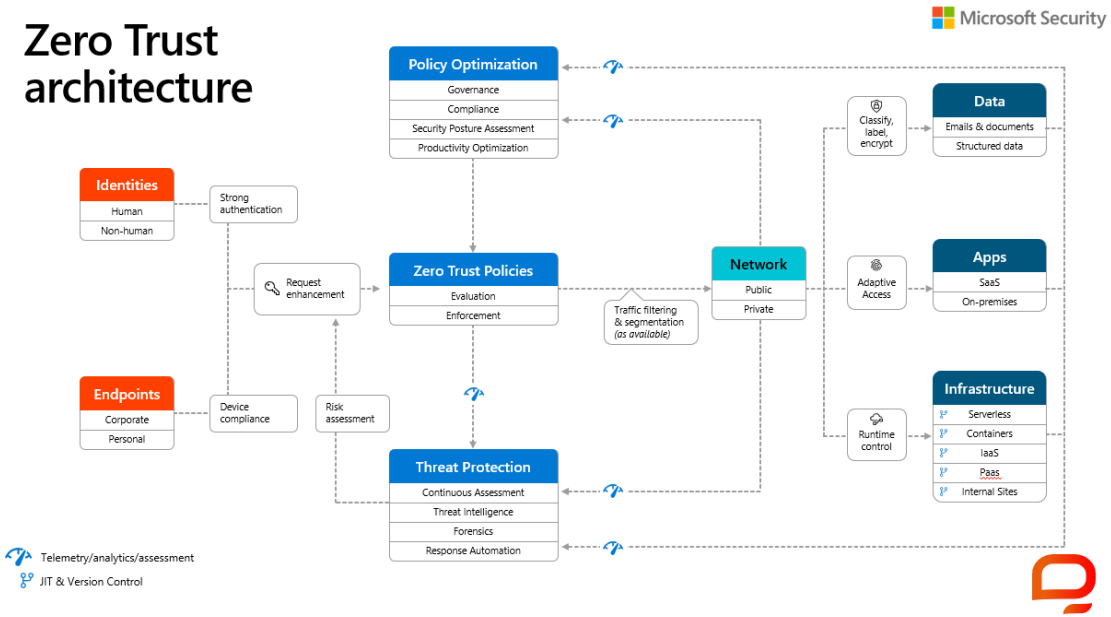
Microsoft Security



Telemetry/analytics/assessment

JIT & Version Control

Was Sie mit Zero Trust verteidigen

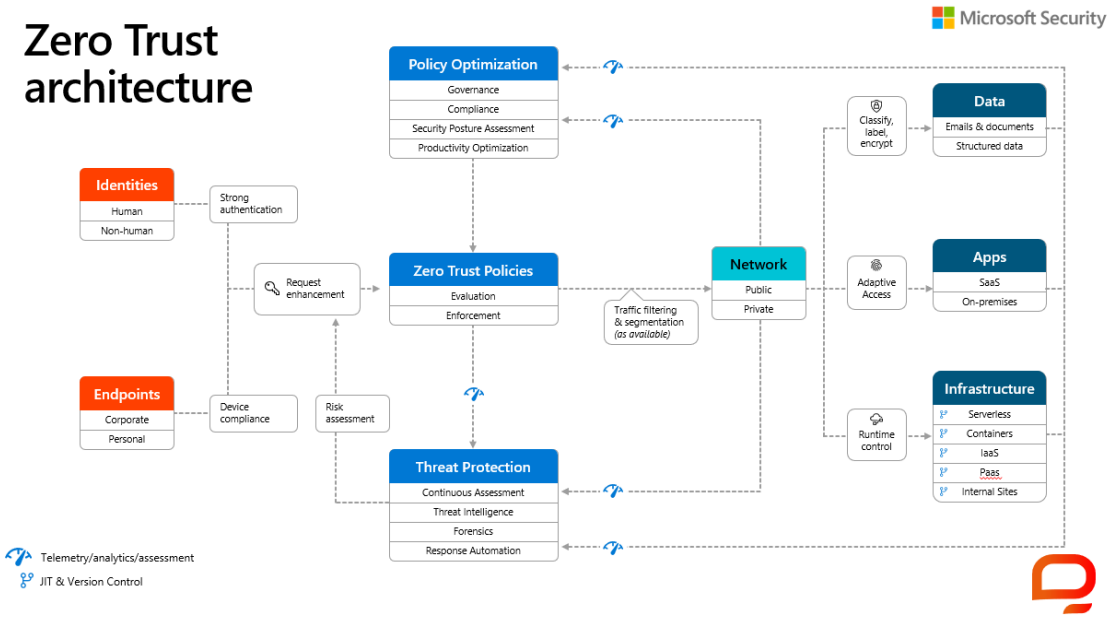


Ein ganzheitlicher Zero-Trust-Ansatz erstreckt sich auf die gesamte digitale Umgebung - einschließlich Identitäten, Endpunkten, Netzwerk, Daten, Anwendungen und Infrastruktur. Die Zero-Trust-Architektur, in der eine umfassende End-to-End-Strategie abgebildet ist, erfordert die Integration aller Elemente.

Identitäten sind die Grundlage der Zero-Trust-Sicherheit. Sowohl menschliche als auch nicht-menschliche Identitäten erfordern eine starke Autorisierung. Die Verbindung mit konformen Geräten erfolgt über persönliche oder firmeneigene Endpunkte, die den Zugriff beide auf der Grundlage strenger Richtlinien und bewährter Zero-Trust-Prinzipien anfordern: explizite Verifizierung, Zugriff mit den geringstmöglichen Berechtigungen und Assume Breach.

Im Rahmen der durchgängigen Richtliniendurchsetzung fängt die Zero-Trust-Richtlinie die Anforderung ab, verifiziert auf der Grundlage der Richtlinienkonfiguration explizit Signale aus den sechs Grundkategorien und setzt den Zugriff mit den geringstmöglichen Berechtigungen durch. Die Signale beziehen sich auf die Benutzerrolle, den Standort, die Gerätekonformität sowie die Vertraulichkeit von Daten und Anwendungen.

Was Sie mit Zero Trust verteidigen

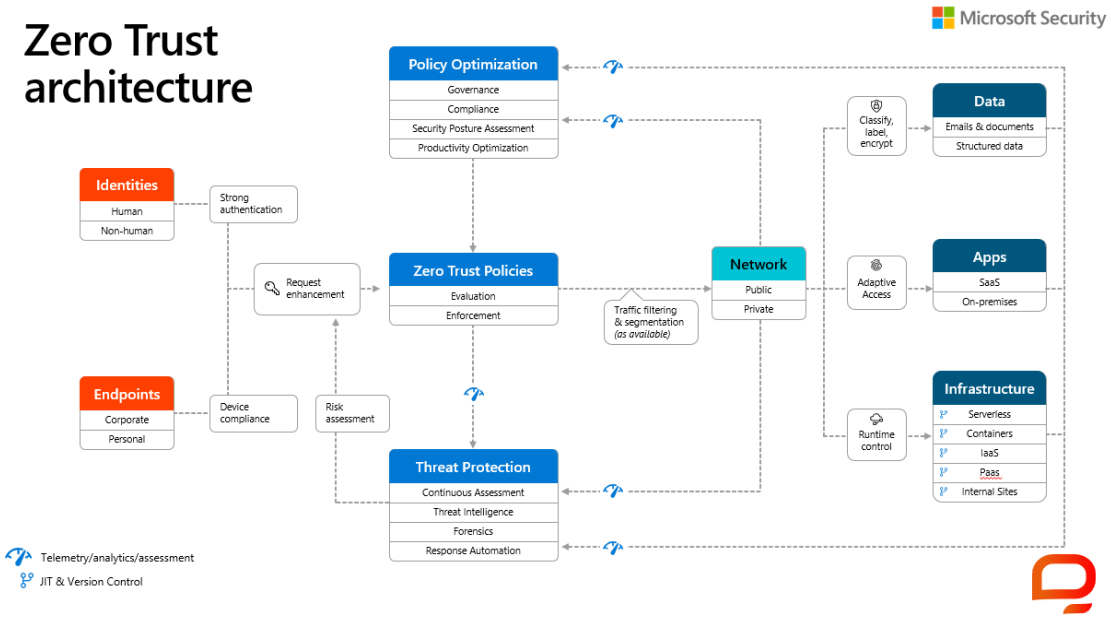


Zusätzlich zu den Telemetrie- und Statusinformationen fließt die Bedrohungsschutz-Risikobewertung in das Richtlinienmodul ein, um automatisch und in Echtzeit auf Bedrohungen zu reagieren. Die Richtlinie wird beim Zugriff durchgesetzt und während der gesamten Sitzung kontinuierlich ausgewertet.

Außerdem wird die Richtlinie durch die Richtlinienoptimierung weiter verbessert. Governance und Compliance sind wichtig für eine erfolgreiche Zero-Trust-Implementierung. Die Bewertung des Sicherheitsstatus und die Produktivitätsoptimierung sind erforderlich, um die Telemetrie in allen Diensten und Systemen zu messen.

Die Telemetrie- und Analysedaten fließen in das Bedrohungsschutzsystem ein. Umfangreiche Telemetrie- und Analysedaten, die mit Threat Intelligence angereichert sind, generieren aussagekräftige Risikobewertungen, die entweder manuell untersucht oder automatisiert werden können. Angriffe erfolgen mit Cloudgeschwindigkeit.

Was Sie mit Zero Trust verteidigen



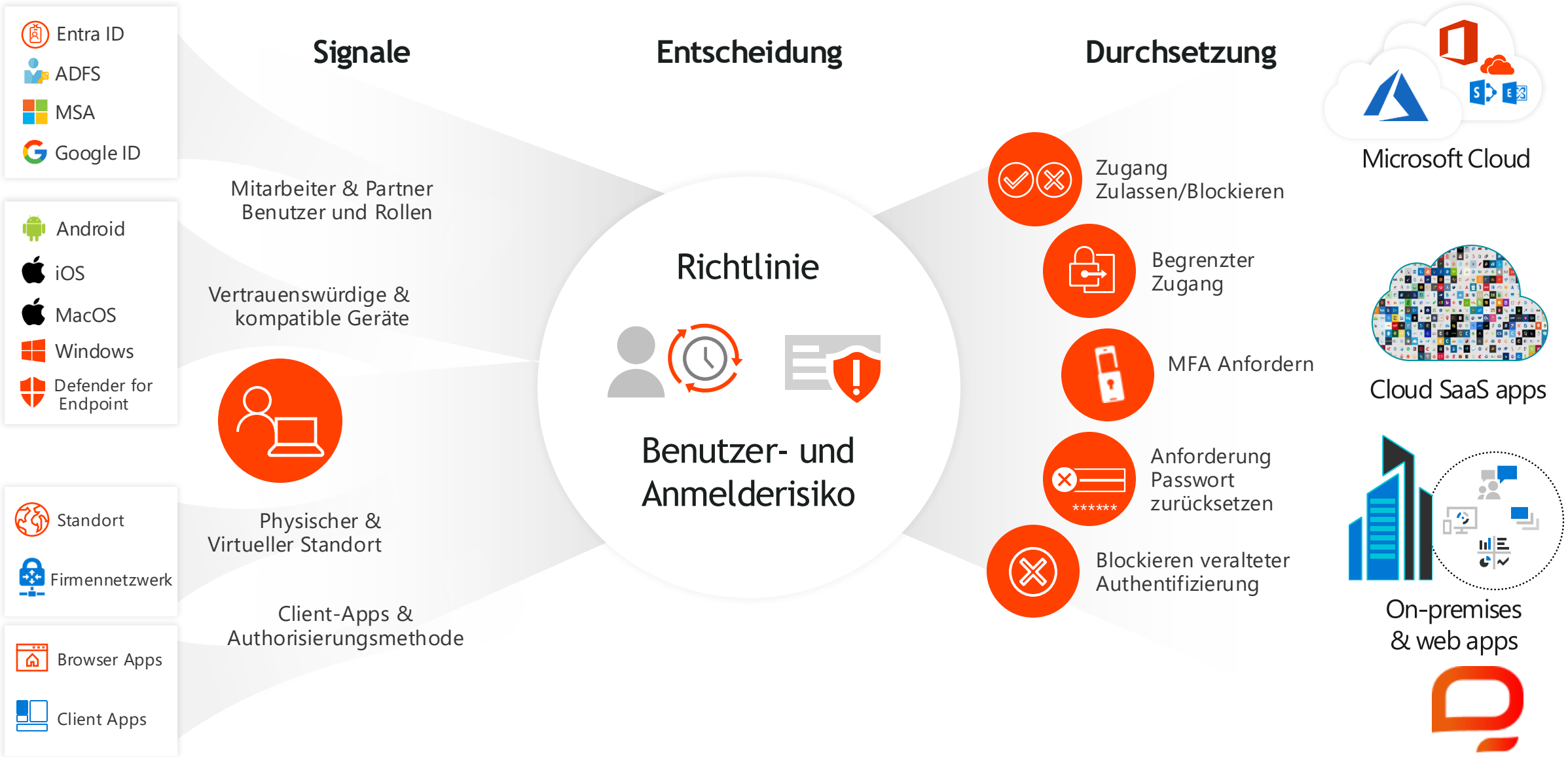
Dasselbe muss auch für die Verteidigungssysteme gelten, denn Menschen können nicht schnell genug reagieren bzw. alle Risiken erkennen. Die Risikobewertung fließt in das Richtlinienmodul ein und ermöglicht so den automatisierten Echtzeit-Bedrohungsschutz sowie bei Bedarf eine zusätzliche manuelle Untersuchung.

Vor der Evaluierung und Durchsetzung der Zero-Trust-Richtlinie findet die Filterung und Segmentierung des Datenverkehrs statt. Erst danach wird der Zugriff auf ein öffentliches oder privates Netzwerk gewährt.

Klassifizierung, Kennzeichnung und Verschlüsselung von Daten sollten auf E-Mails, Dokumente und strukturierte Daten angewendet werden. Der Zugriff auf Apps erfolgt adaptiv, sowohl bei SaaS- als auch bei lokalen Apps. Die Laufzeitsteuerung wirkt sich auf die Infrastruktur mit serverlosen, containerbasierten, IaaS-, PaaS- und internen Websites aus, wobei JIT (Just-in-Time) und Versionskontrolle aktiv eingesetzt werden.

Zum Schluss werden Telemetrie- und Analysedaten sowie Bewertungen aus dem Netzwerk, den Daten und Anwendungen sowie der Infrastruktur in die Richtlinienoptimierungs- und Bedrohungsschutzsysteme zurückgeführt.

Kontrollieren Sie den Zugriff mit intelligenten Richtlinien und Risikobewertungen



Nutzen Sie die Vorteile durch die Absicherung mit Zero-Trust

Wir beraten Sie zu den relevanten Bestandteilen von Microsoft 365 und erhöhen mit Ihnen die Wertschöpfung Ihrer Investition in Microsoft Clouddienste

Entra ID

Entra ID schützt Ressourcen und Daten mit starker Authentifizierung, Single Sign-On (SSO), kennwortloser und Multi-Faktor-Authentifizierung (MFA) sowie eigenständige Kennwortzurücksetzung

Bedingter Zugriff

adaptive risikobasierte Zugriffsrichtlinien, ohne das Benutzererlebnis einzuschränken

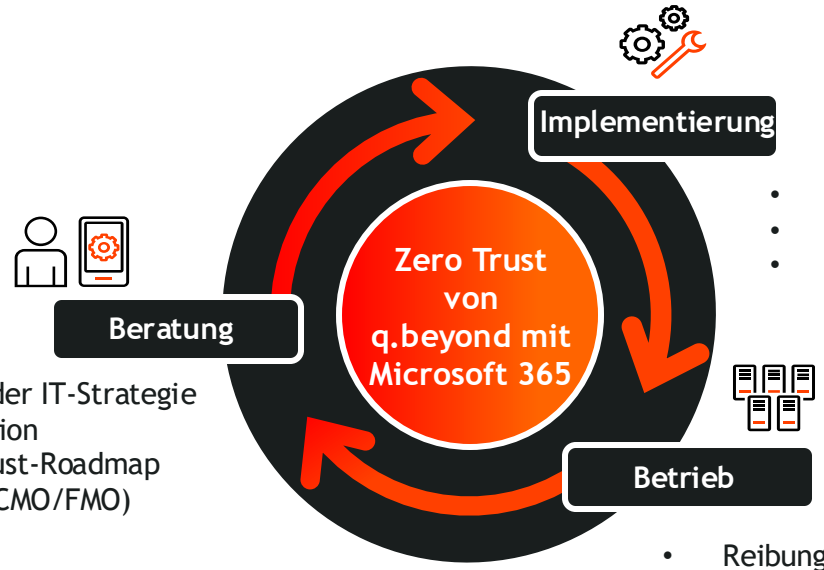
Microsoft Intune

Verwaltung und Überwachung (Konformitätsprüfung) von Geräten. Konfiguration und Anwendung von Richtlinien für Benutzer und Geräte.

q.beyond

Microsoft 365

Die richtige Leistung für jeden Abschnitt der Modernisierung



- Gemeinsame Planung der IT-Strategie
- Analyse Bestandssituation
- Erstellung der Zero-Trust-Roadmap
- Zero-Trust Workshop (CMO/FMO)

- Sichere Umsetzung Ihrer Roadmap
- Schulungen für die Mitarbeitenden
- Durchführung von Tests (Pilotphase) für einen reibungslosen Betrieb

- Reibungsloser Betrieb Ihrer Identitäten und Geräte
- Überwachung, Wartung und Optimierung der Zugriffsrichtlinien
- Regelmäßige Beratung zur Optimierung des Nutzens der cloudbasierten Lösungen

Wir entwerfen mit Ihnen den Bereitstellungsplan für Zero-Trust und begleiten Sie zuverlässig und transparent als kompetenter Partner bei Umsetzung und Betrieb.

q.beyond macht Sie erfolgreich in der digitalen Welt.

Prozess-, Geschäfts- und Servicemodelle rund um Cloud, SAP, Microsoft, Data Intelligence, Security und Softwareentwicklung

Die richtige Leistung für jeden Digitalisierungsabschnitt

Beratung > Entwicklung > Betrieb

Von Mittelstand zu Mittelstand

Vielen Dank!

Simon Taylor
Business Development Microsoft

simon.taylor@qbeyond.de
www.qbeyond.de

q.beyond


q.beyond
expect the next