

Paradigmenwechsel in der IT-Sicherheit

Never trust, always verify: Zero-Trust Framework Microsoft 365

Wer bin ich?

Jens Kersten

Cloud Presales Engineer

bei der TD Synnex seit März 2019



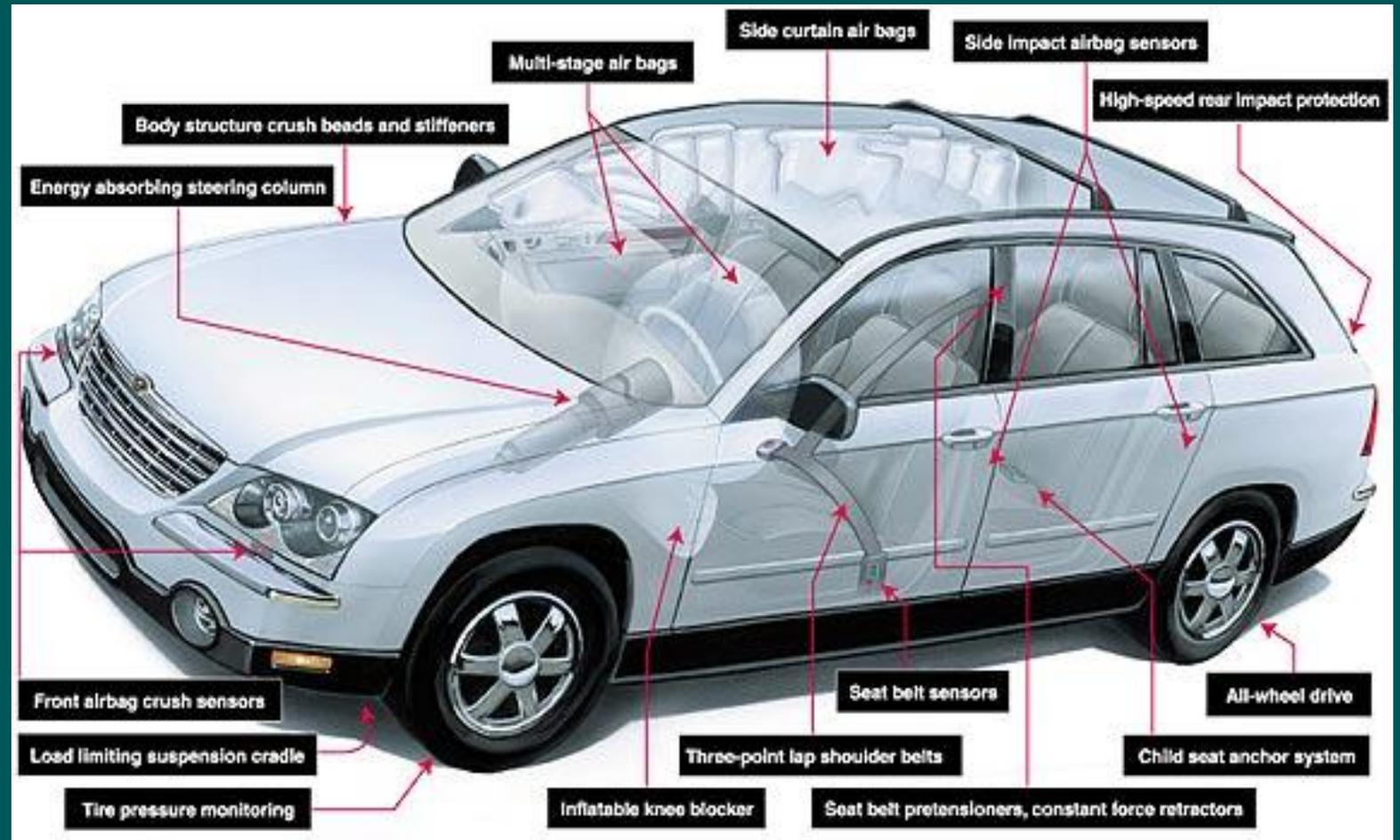
Jens Kersten
Cloud PreSales Engineer
TD SYNnex GmbH & Co. oHG
Kistlerhofstrasse 75
81379 München
E-mail jens.kersten@tdsynnex.com

Gefahrenabwehr im Straßenverkehr - Vergangenheit



Die sich verändernde Bedrohungslandschaft erfordert neue Sicherheitsfunktionen!

Gefahrenabwehr im Straßenverkehr— Heute





Modernes Arbeiten ist jetzt hybrides Arbeiten

Zu Hause



Unterwegs

Ihr Büro ist
dort, wo Sie
wollen



Hybrides Arbeiten



Bei der Arbeit

Hybrides Arbeiten – Ja, aber war da nicht noch was?

Sicherheitsbedrohungen

Da Sicherheitsbedrohungen in Umfang und Schwere immer weiter zunehmen, migrieren viele Unternehmen zur Risikominimierung in die Cloud. Anbieter öffentlicher Clouds bieten umfangreiche Ressourcen [für den Schutz vor Bedrohungen](#) – mehr als es den meisten Unternehmen möglich ist zu investieren.

Mythen und ihre Fakten

Cyberangriffe häufen sich immer mehr.
Die Angriffsfläche vergrößert sich durch die fortschreitende Digitalisierung
ebenso. Dabei müssen IT-Abteilungen und Experten mithalten können.
Das wird durch Mythen und Missverständnisse jedoch nur erschwert.

Mein Unternehmen ist für Angriffe uninteressant

Cybergefahren kommen von außerhalb

Sicherheit ist Aufgabe der IT

-> Mehr Sicherheit heißt mehr Aufwand?

Gängige Bedrohungen



Datenpanne

Inklusive:

- Phishing
- Spear-Phishing
- Tech-Support-Betrug
- Einschleusung von SQL-Befehlen
- Malware zum Ausspähen von Kennwörtern und Bankinformationen



Wörterbuchangriff

Hierbei handelt es sich um eine Form von Identitätsangriffen.

Ein Hacker versucht, eine Identität zu stehlen, indem eine Vielzahl von bekannten Kennwörtern ausprobiert wird.

Wörterbuchangriffe werden auch als „Brute-Force-Angriffe“ bezeichnet.



Ransomware

Dies ist eine Form von Malware, mit der Dateien und Ordner verschlüsselt werden.

Sie zielt darauf ab, Geld von den Opfern zu erbeuten.



Störangriffe

Ein verteilter Denial-of-Service-Angriff (DDoS) zielt darauf ab, die Ressourcen einer Anwendung auszuschöpfen.

DDoS-Angriffe können jeden Endpunkt zum Ziel haben.

Andere gängige Bedrohungen sind Coinminer, Rootkits, Trojaner, Würmer sowie Exploits und Exploitkits.

Over 620 Million Ransomware Attacks Detected in 2021 - Infosecurity Magazine (infosecurity-magazine.com)



Angriffszeitraum



Erster Host
Kompromittiert



Domain Admin
Kompromittiert



Angriff
Entdeckt

Recherche und Vorbereitung

Angreifer unentdeckt (Datenverlust)



24–48 Stunden



Mehr als 200 Tage* (variiert je nach Industry)

Angriff



Angreifer nutzen jede Schwachstelle aus.

Zielen auf Informationen von jedem Gerät oder Dienst

Ziel AD und Identitäten



AD steuert den Zugriff auf Unternehmensressourcen.

Angreifer richten sich häufig gegen AD- und IT-Admins

Angriff nicht erkannt



Aktuelle Werkzeuge verfehlen die meisten Angriffe.

Du könntest angegriffen (oder kompromittiert) sein.

Reaktion und Wiederherstellung

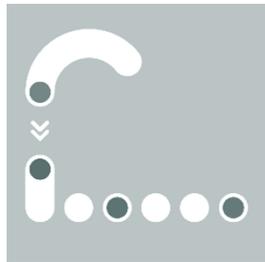


Die Reaktion erfordert fortgeschrittenes Fachwissen und Werkzeuge. Erfolgreiche Wiederherstellung ist Teuer und herausfordernd

„Alte Welt“ Implicit Trust



Schutz durch Unternehmens-Firewall



Sicherheitsanomalien werden geprüft

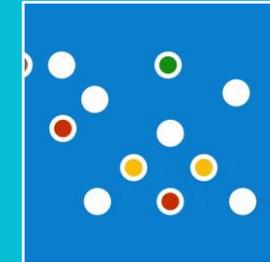


Modernes Arbeiten nur bedingt möglich

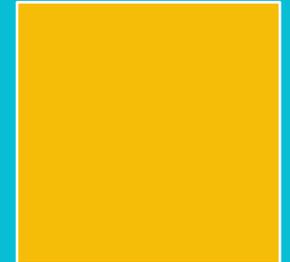
„Hybride Welt“ Zero Trust



Vielzahl an Endgeräten



Mobiles Arbeiten an jedem beliebigen Ort (produktiv & sicher)



Vernetzte Welt

ASSUME BREACH

PROTECT
Security Development Lifecycle
Threat Modeling
Code Review
Security Testing
Network/User/Data/System security



DETECT
Auditing and Certification
Live Site Penetration Testing
Centralized Logging and Monitoring
Fraud and Abuse Detection

LEARN
Post-Breach Assessment

RESPOND
Breach Containment
Coordinated Security Response
Customer Notification

Microsoft Zero-Trust-Prinzipien

Leitfaden für die technische Architektur



Explizit verifizieren

Überprüfen Sie **immer alle verfügbaren Datenpunkte**, einschließlich

- Benutzeridentität und Standort
- Gerätezustand
- Dienst- oder Workloadkontext
- Datenklassifizierung
- Anomalien



Verwenden des Zugriffs nach dem Prinzip der geringsten Rechte

Um sowohl Daten als auch Produktivität zu sichern, beschränken Sie den Benutzerzugriff mithilfe von

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors

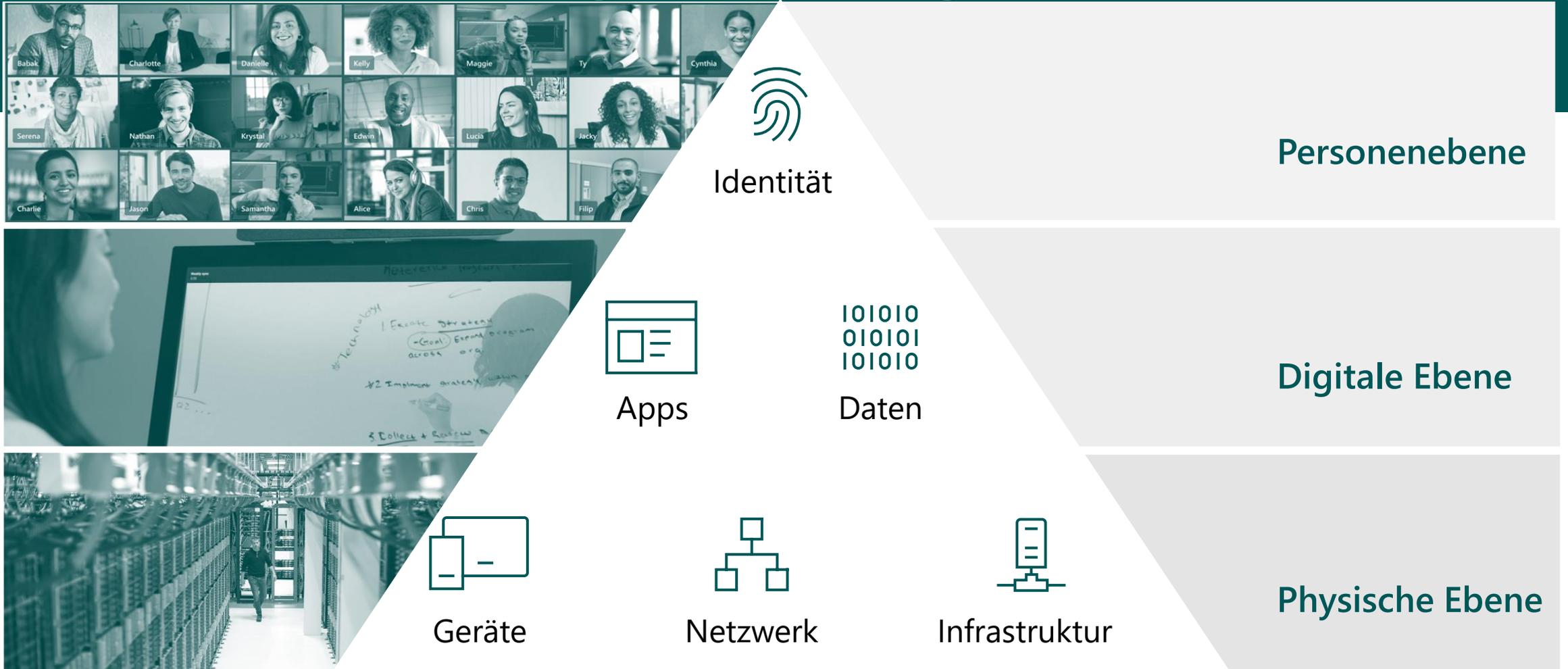


Verstoß annehmen

Minimieren Sie den Explosionsradius bei Verletzungen / Einbrüchen und verhindern Sie die Ausbreitung durch

- **Segmentierung** des Zugriffs nach Netzwerk, Benutzer, Geräten und App-Bewusstsein.
- **Verschlüsselung** aller Sitzungen Ende-zu-Ende.
- Nutzen Sie **Analysen** zur Erkennung von Bedrohungen, zur Transparenz der Haltung und zur Verbesserung der Abwehr

Zero Trust über den gesamten digitalen Bestand hinweg



Authentifizierung

Verwenden Sie intelligente Schutzrichtlinien und Risikobewertungen, um Bedrohungen zu blockieren.

81%

aller Hacks durch gestohlene oder schwache Passwörter



Microsoft Authenticator



Windows Hello



FIDO2 Security key



Push Notification



Soft Tokens OTP



Hard Tokens OTP



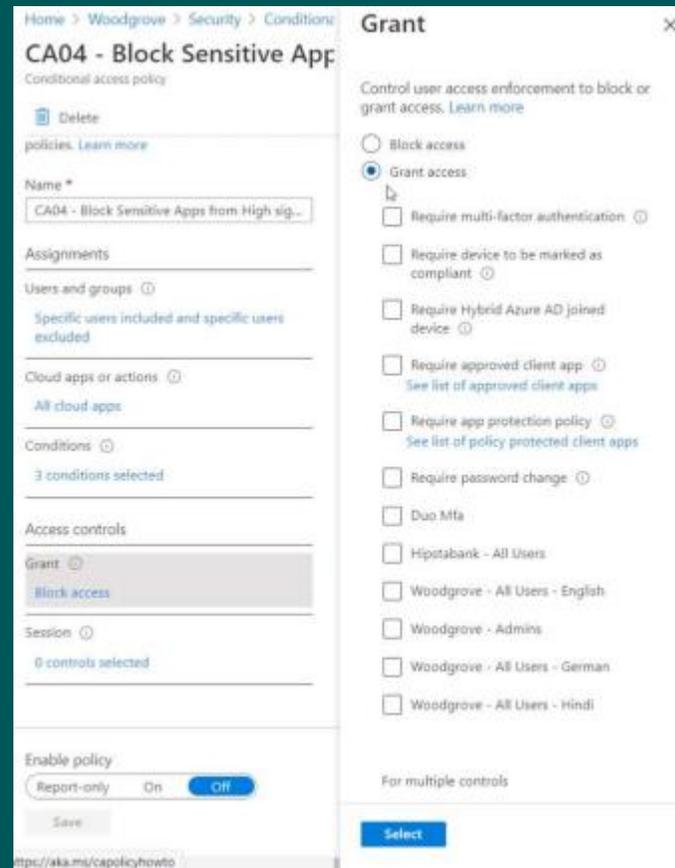
SMS, Voice

Multi-Faktor-Authentifizierung verhindert 99,9% der Identitätsangriffe.

Identity Protection mit Conditional Access



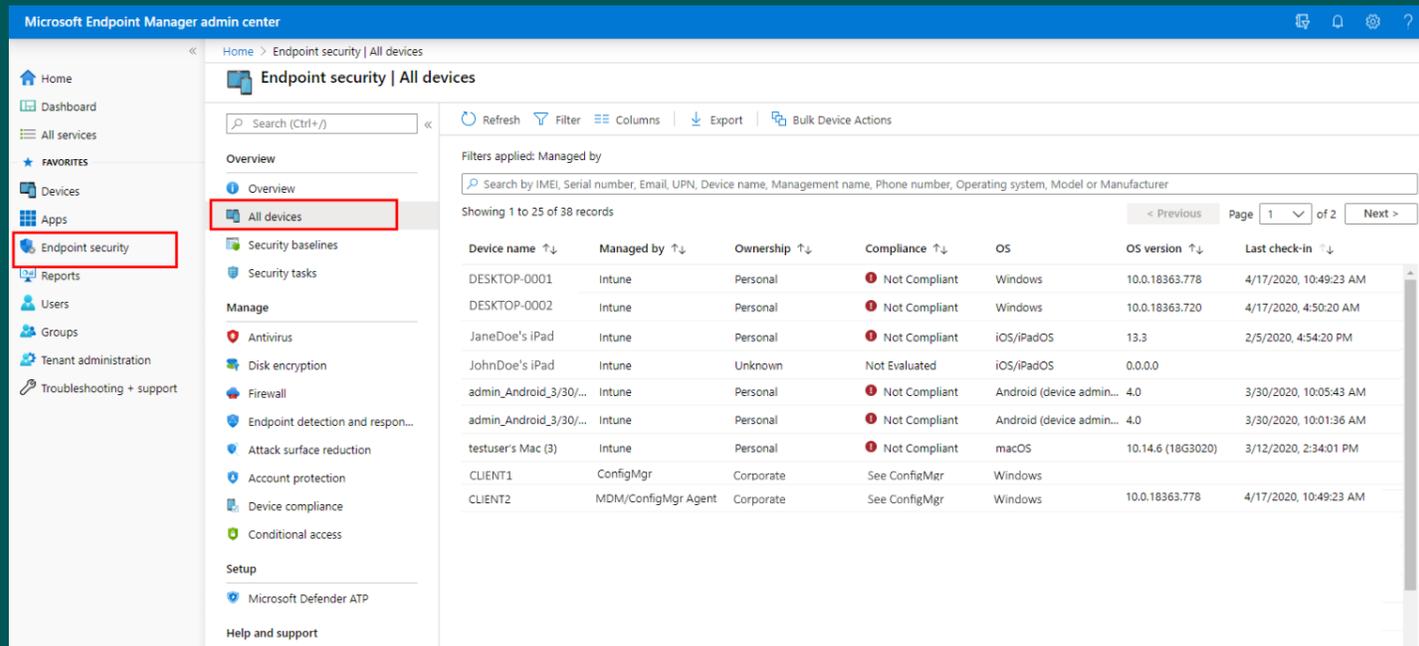
Conditional access



- Festlegen von Richtlinien zur Bewertung der Risikostufen
- Risikokriterien können sein, z.B.:
 - Benutzer oder Anmeldeverhalten
 - Geräteplattform
 - Anmeldeorte
 - Anwendungen
- Zugriffsrichtlinien werden in Echtzeit durchgesetzt, z.B. um Zugriffe zu blockieren, Kennworrücksetzung zu verlangen, Zugriff zu gewähren, zusätzlichen Authentifizierungsfaktor zu verlangen oder beispielsweise auf reine Ansichtsrechte zu beschränken.

Endgeräte schützen mit dem MS Endpoint Manager

Wenn Benutzer auf Ressourcen, Daten und Anwendungen, zugreifen, gehören die Endgeräte möglicherweise nicht zu Ihrem Unternehmen und werden nicht von diesem verwaltet. Wenn die Endgeräte nicht auf dem neuesten Stand sind oder nicht angemessen geschützt werden, besteht die Gefahr, dass Daten von unbekanntem Anwendungen oder Diensten exfiltriert werden. Mit Microsoft Endpoint Manager können Sie sicherstellen, dass die Geräte und die auf ihnen installierten Anwendungen die Anforderungen Ihrer Sicherheits- und Compliance-Richtlinien erfüllen, unabhängig davon, ob das Gerät Ihrem Unternehmen oder dem Benutzer gehört. Dieser Schutz gilt unabhängig davon, von wo aus das Gerät eine Verbindung herstellt - sei es innerhalb der Netzwerk Grenzen, einschließlich über ein VPN, in einem Heimnetzwerk oder im öffentlichen Internet.



Microsoft Endpoint Manager admin center

Home > Endpoint security | All devices

Endpoint security | All devices

Search (Ctrl+F)

Refresh Filter Columns Export Bulk Device Actions

Filters applied: Managed by

Search by IMEI, Serial number, Email, UPN, Device name, Management name, Phone number, Operating system, Model or Manufacturer

Showing 1 to 25 of 38 records

Device name	Managed by	Ownership	Compliance	OS	OS version	Last check-in
DESKTOP-0001	Intune	Personal	Not Compliant	Windows	10.0.18363.778	4/17/2020, 10:49:23 AM
DESKTOP-0002	Intune	Personal	Not Compliant	Windows	10.0.18363.720	4/17/2020, 4:50:20 AM
JaneDoe's iPad	Intune	Personal	Not Compliant	iOS/iPadOS	13.3	2/5/2020, 4:54:20 PM
JohnDoe's iPad	Intune	Unknown	Not Evaluated	iOS/iPadOS	0.0.0.0	
admin_Android_3/30/...	Intune	Personal	Not Compliant	Android (device admin...	4.0	3/30/2020, 10:05:43 AM
admin_Android_3/30/...	Intune	Personal	Not Compliant	Android (device admin...	4.0	3/30/2020, 10:01:36 AM
testuser's Mac (3)	Intune	Personal	Not Compliant	macOS	10.14.6 (18G3020)	3/12/2020, 2:34:01 PM
CLIENT1	ConfigMgr	Corporate	See ConfigMgr	Windows		
CLIENT2	MDM/ConfigMgr Agent	Corporate	See ConfigMgr	Windows	10.0.18363.778	4/17/2020, 10:49:23 AM

Conditional Access – Block PC w/ Ransomware

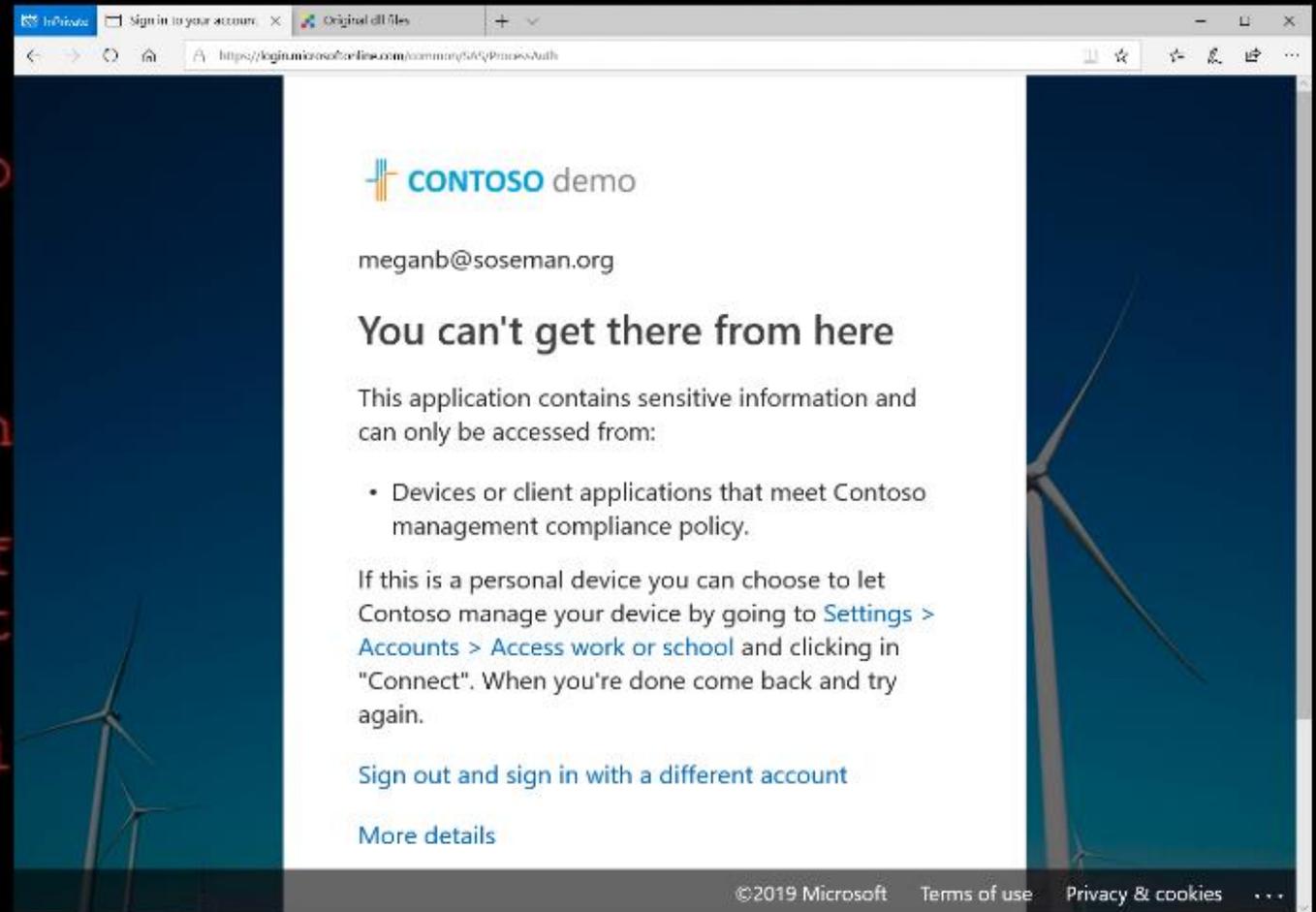
Ooops, your important files are encrypted.

If you see this text, but do then your antivirus removed it from your computer.

If you need your files you h

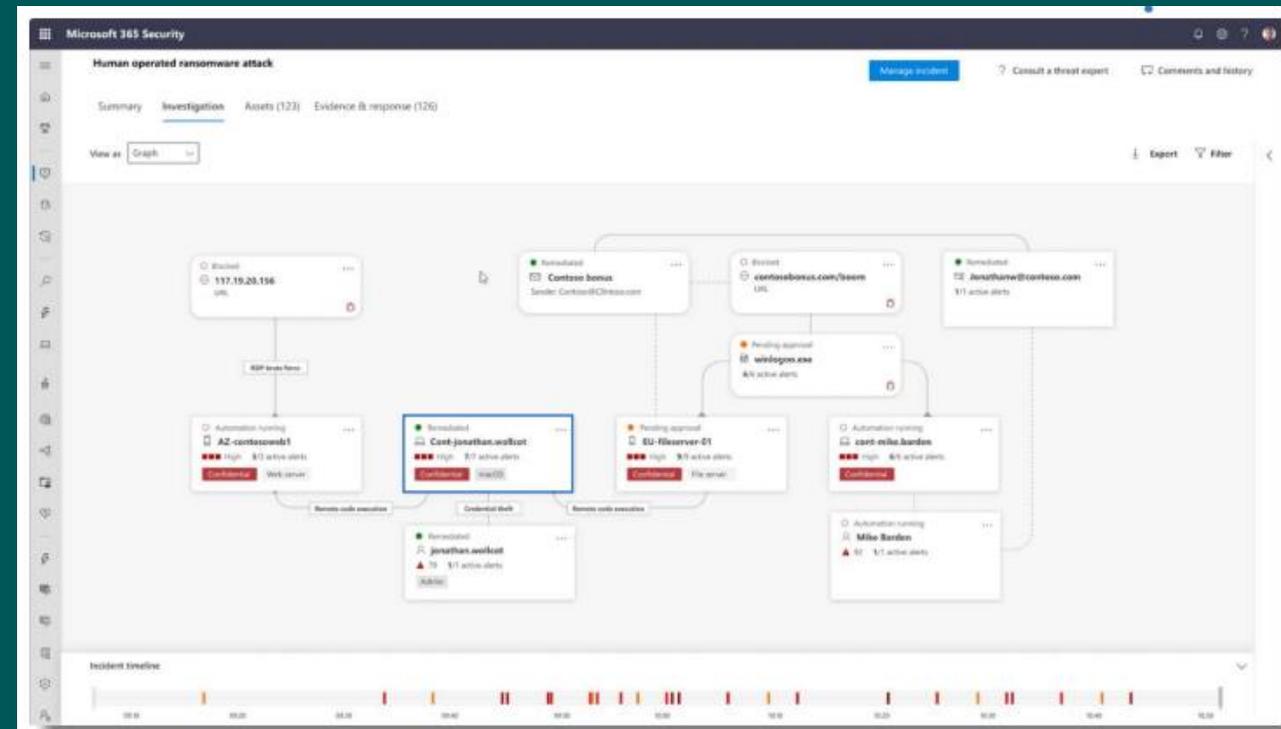
Please find an application f any folder or restore from t

Run and follow the instructi



Microsoft Defender

Microsoft Defender mit seinen erweiterten Erkennungs- und Reaktionskontrollen (Extended Detection and Response oder XDR) kann auf einem Gerät entdeckte Sicherheitslücken erkennen, eindämmen und das Gerät wieder in einen vertrauenswürdigen Zustand versetzen, bevor es wieder eine Verbindung zu ihrem Netzwerk oder Ressourcen herstellen darf.



Microsoft Security im Überblick

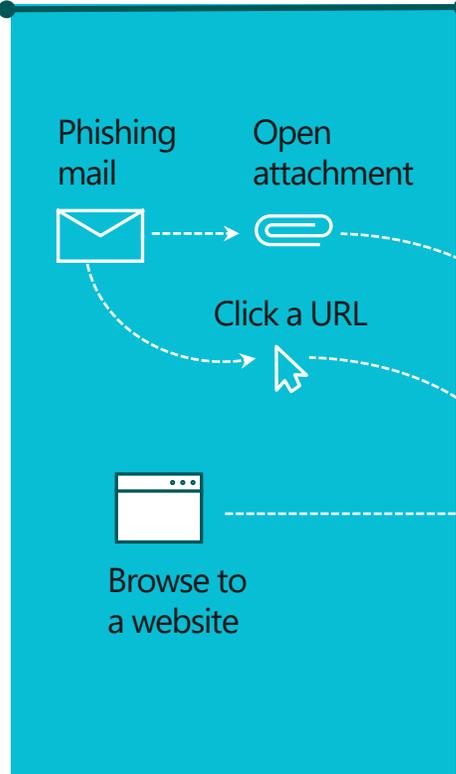
	Identity and access management	Threat protection	Cloud security	Information protection & governance	Risk management	Compliance management
Microsoft 365	Azure AD Premium • Azure AD Identity Governance	Microsoft 365 Defender <ul style="list-style-type: none"> • Microsoft Defender for Endpoint • Microsoft Defender for Office 365 • Microsoft Defender for Identity • Microsoft Defender for Cloud Apps 	Microsoft Defender for Cloud Apps	Microsoft Information Protection	Insider Risk Management	Compliance Manager
	Microsoft Endpoint Manager			Microsoft Information Governance	eDiscovery	
		Microsoft Data Loss Prevention	Advanced Audit			
		Records Management	Communication Compliance			
		Threat and Vulnerability Management			Information Barriers	
					Privileged Access Management	
Azure	Azure AD B2C	Microsoft Defender for Cloud	Microsoft Defender for Cloud	Azure Purview		
	Azure AD Domain Services	Microsoft Sentinel (SIEM)	Azure Firewall Azure DDoS Protection Azure Bastion			
	Azure Key Vault	Azure AD Identity Protection	Azure Web App Firewall Azure Front Door			
		Microsoft Defender for IoT				
		Azure Sphere				

+ Partner Lösungen

Schutz entlang der gesamten Angriffslinie

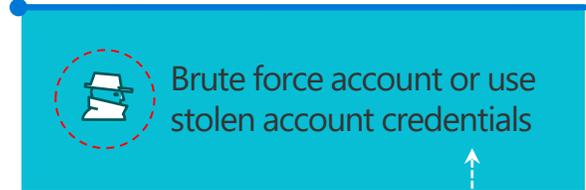
Microsoft 365 Defender

Malware detection, safe links, and safe attachments



Azure AD Defender for Identity

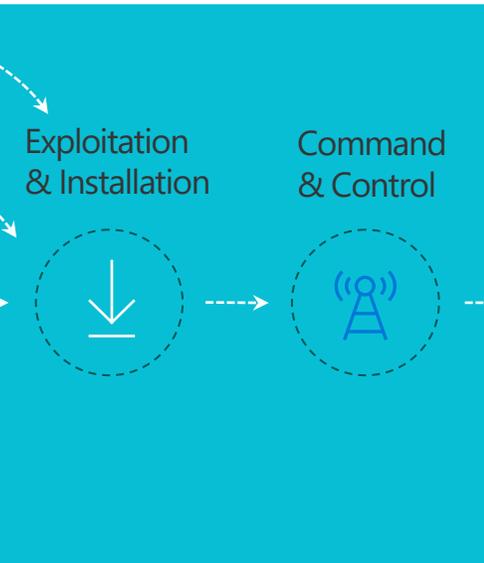
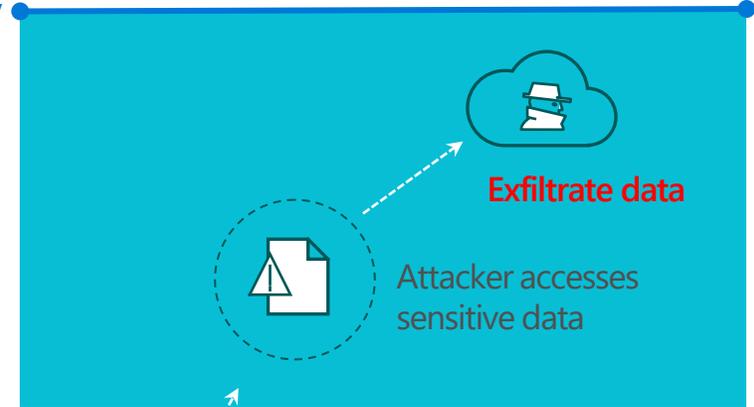
Identity protection & conditional access



Defender for Cloud App Security

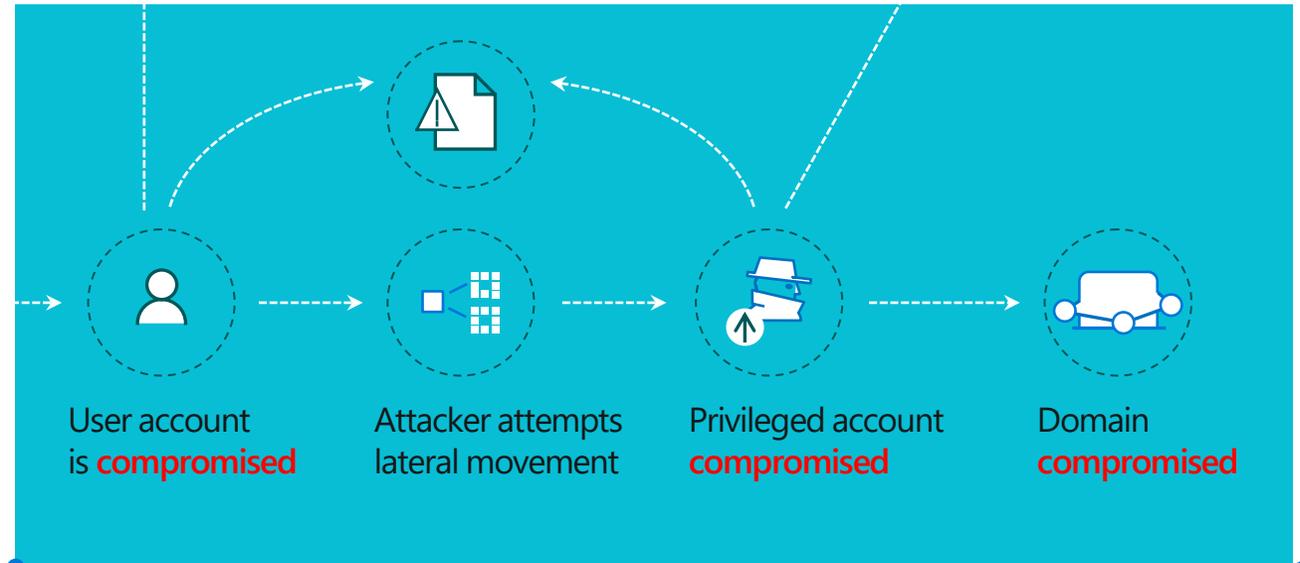
Extends protection & conditional access to other cloud apps

Attacker collects **reconnaissance & configuration data**



Microsoft Defender for Endpoints

Endpoint Detection and Response (EDR) & End-point Protection (EPP)



Defender for Cloud

Identity protection

Klassifizierung von Daten in O/M 365

Data Loss Prevention (DLP)

Was ist das?

Mit Data Loss Prevention (DLP)-Richtlinien können Sie verhindern, dass sensible Informationen wie Kreditkartendaten, Sozialversicherungsnummern oder Gesundheitsdatensätze unbeabsichtigt mit nicht autorisierten Personen außerhalb des Unternehmens geteilt werden.

Das Wichtigste auf einen Blick

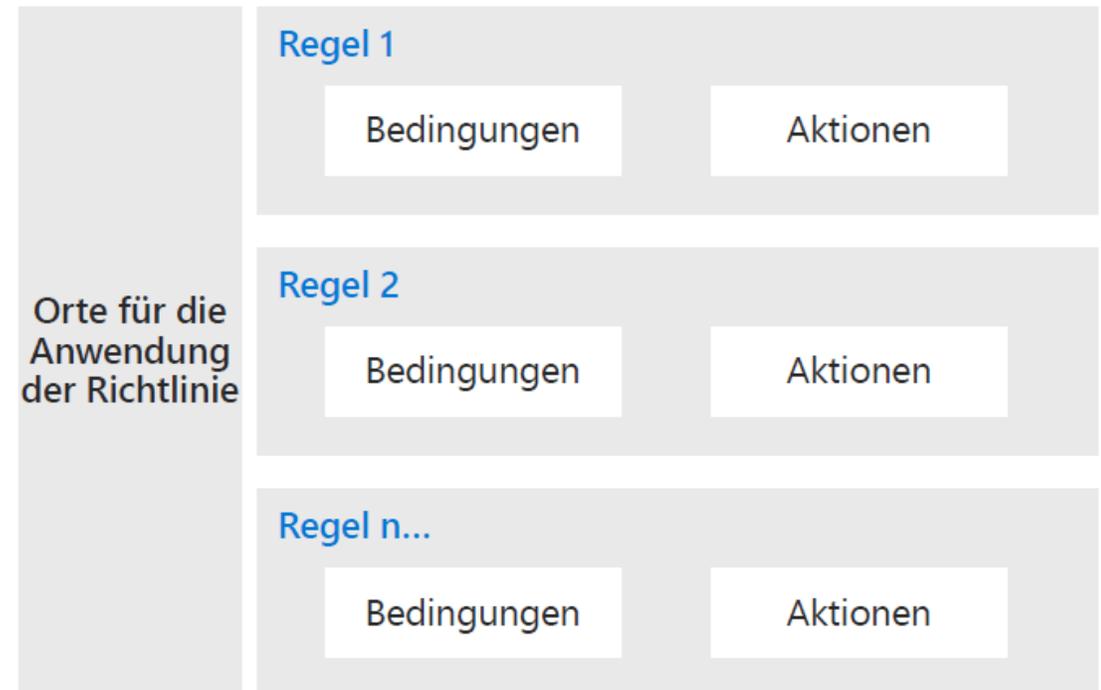
Eine DLP-Richtlinie basiert auf wesentlichen Parametern:

- **Wo** Inhalte geschützt werden sollen – also an Orten wie Exchange Online, SharePoint Online und OneDrive for Business-Websites
- **Wann und wie** Inhalte geschützt werden sollen – und zwar mithilfe von Regeln, die aus zwei Komponenten bestehen:

Bedingungen, die der jeweilige Inhalt erfüllen muss, bevor die Regel angewendet wird. Beispiel: Es sollen nur Inhalte nachverfolgt werden, die Sozialversicherungsnummern enthalten und an Personen außerhalb des eigenen Unternehmens weitergeleitet werden.

Aktionen, die durch die Regel automatisch angewendet werden sollen, wenn Inhalte ermittelt werden, die den Bedingungen entsprechen. Beispiel: Sperre des Zugriffs auf das Dokument und Aussendung einer E-Mail-Benachrichtigung an den Nutzer und an den Compliance-Beauftragten des Unternehmens.

Data Loss Prevention-Richtlinie



Azure Information Protection (AIP)

Was ist das?

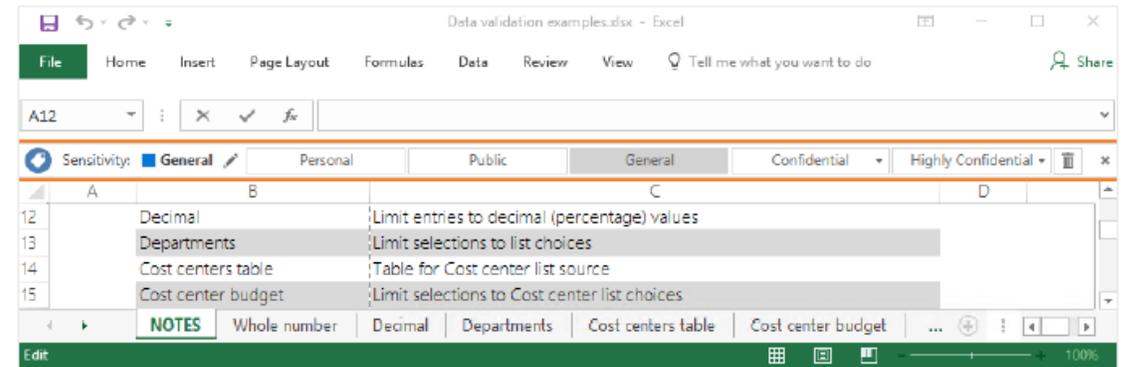
Azure Information Protection (AIP) ist eine cloudbasierte Lösung, mit der Unternehmen ihre Dokumente und E-Mails klassifizieren, kennzeichnen und schützen können.

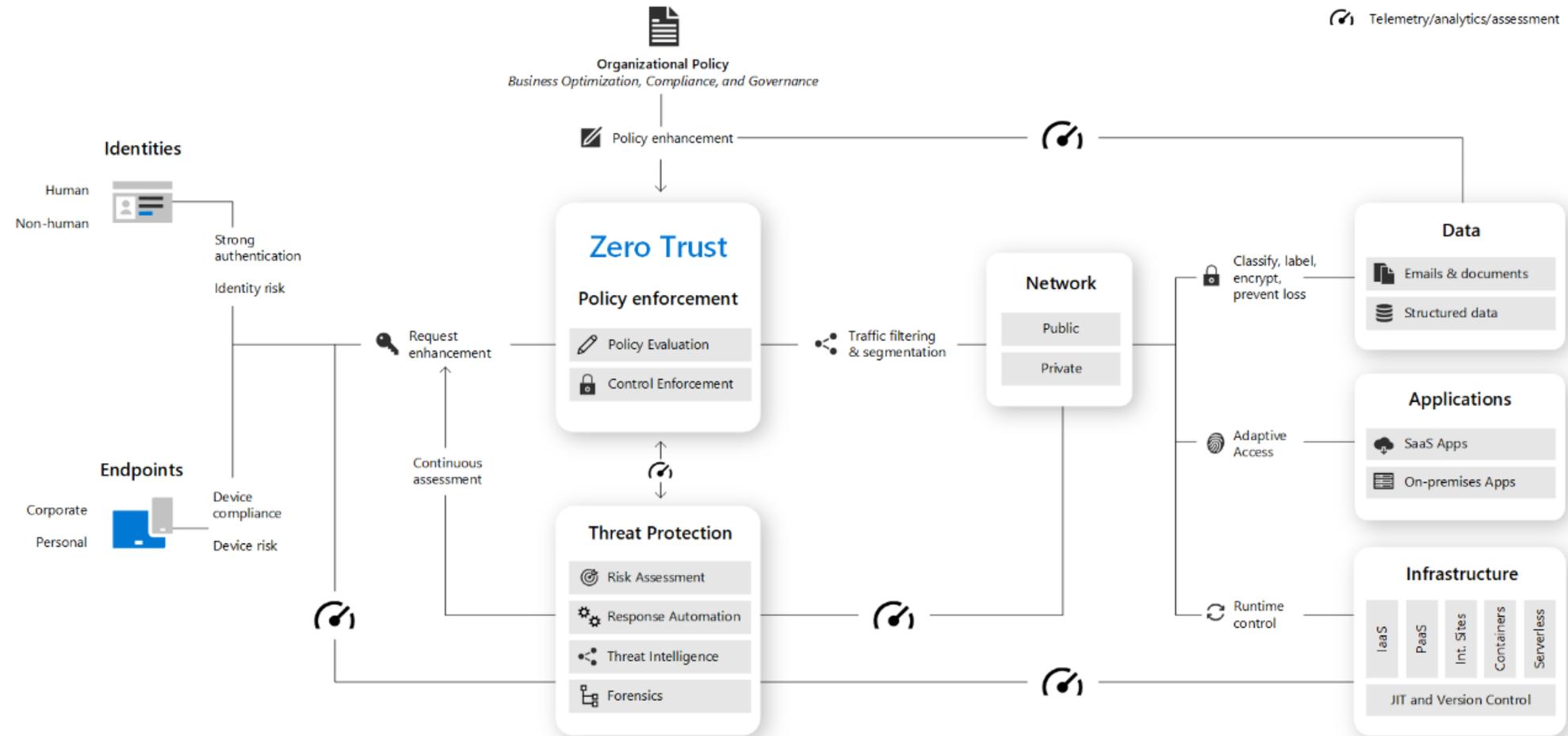
Das Wichtigste auf einen Blick

AIP unterstützt die Klassifizierung von Daten nach dem Grad ihrer Vertraulichkeit. Sie konfigurieren Richtlinien, um Daten entsprechend zu klassifizieren, zu kennzeichnen und zu schützen.

Die Klassifizierung und der Schutz von Informationen folgen den Daten, sodass sichergestellt wird, dass sie unabhängig davon, wo sie gespeichert werden oder mit wem sie ausgetauscht werden, stets geschützt bleiben. Sie können festlegen, wer auf Daten zugreifen kann und welche Aktionen ausgeführt werden können. So kann definiert werden, dass Informationen angezeigt und bearbeitet werden dürfen, aber nicht gedruckt oder weitergeleitet werden können.

AIP ist in Microsoft 365 Business standardmäßig mit einem vordefinierten Set von Kennzeichnungen (Labels) aktiviert.





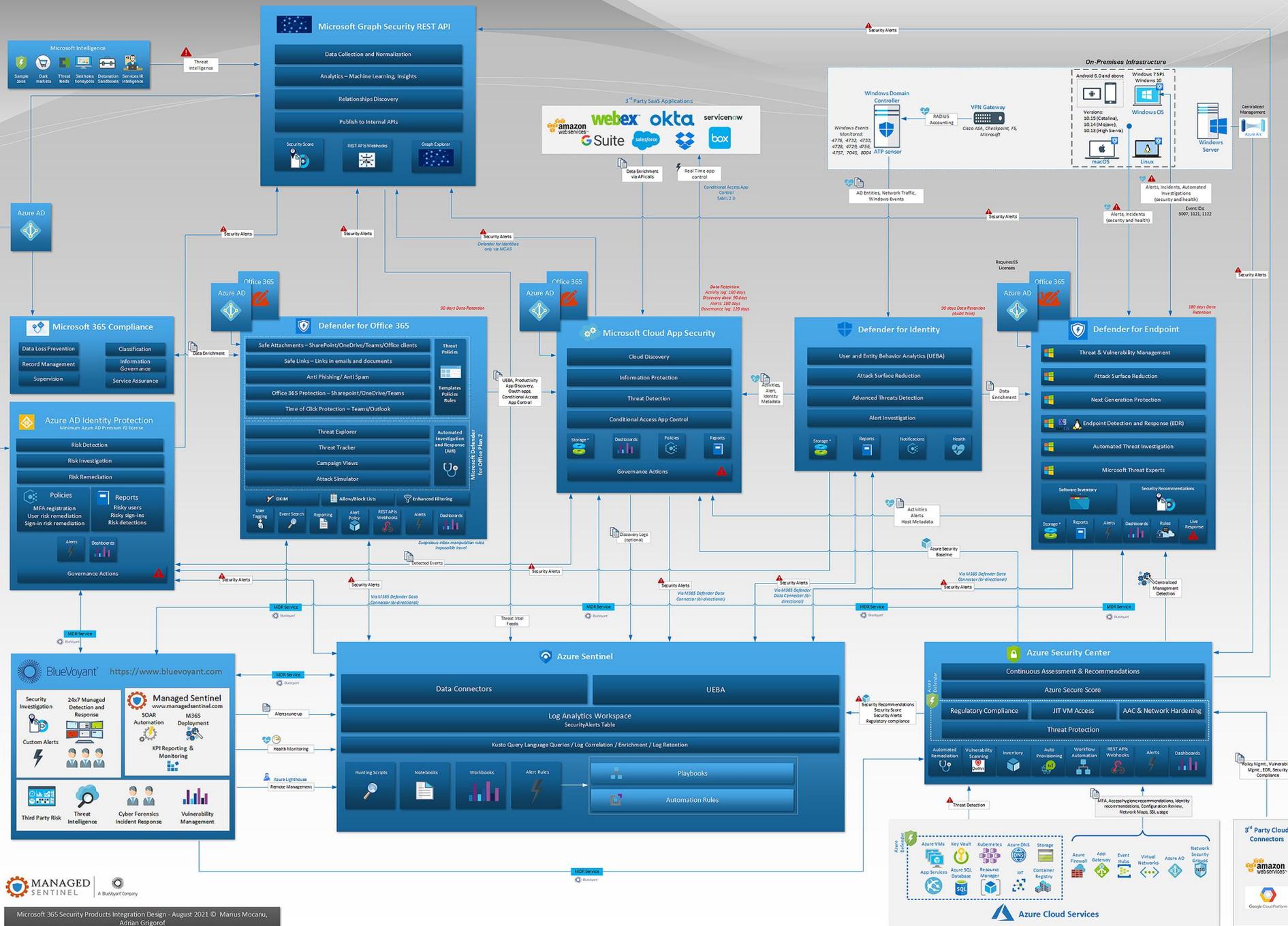
- Security posture assessment
- User experience optimization

Mehr als 3.500 Sicherheitsexperten im **Cyber Defense Operations Center**, der Digital Crimes Unit (DCU) und dem **Microsoft Threat Intelligence Center**, sind täglich für Cybersicherheit im Einsatz. Im Kampf gegen Cybercrime setzt Microsoft auf intelligente Technologien wie erweiterte KI, um täglich **6,5 Billionen Signale** aus der ganzen Welt auf Gefahren zu analysieren, Bedrohungen zu erkennen und Maßnahmen zu ergreifen.



Microsoft ist eine Security Firma





Hero SKU - Microsoft 365 Business Premium

Mit einer Komplettlösung für Unternehmen überall sicher arbeiten

Apps und Dienste für Desktop, Web und Mobilgeräte



Outlook



OneDrive



Word



Excel



PowerPoint



SharePoint



Microsoft Teams



Exchange



Publisher (nur PC)



Access (nur PC)



Intune



Microsoft Defender



Azure Information Protection



Azure AD Premium P1



Azure Virtual Desktop

**Vielen Dank und bleiben
Sie Sicher!**

