BRAIN SHARE
SWS COMPUTERSYSTEME AG

Microsoft Zero Trust

Vertrauen Sie nur auf Fakten und

schützen sie Ihre Daten

IT for innovators.
Member of ACP Group

Oliver Hien

Senior Consultant Datacenter

Microsoft Security, Messaging

Andreas Wach

Cloud Solution Architect

Security, Compliance & Identity

Admin und CISO

Harry Bo

Administrator / Head of IT

Verantwortlich für alles, was einen Stromstecker hat

Heinz Elmann

Chief Information Security Officer (CISO)

Verantwortlich für alles, was Security betrifft

Anforderungen Admin

Wir stehen vor neuen Herausforderungen

User sind nicht nur Mitarbeiter – sondern auch Kunden und Partner

User wollen mit eigenen Geräten von überall aus arbeiten

Die Anzahl an Cloud-Apps wird immer mehr

Immer mehr Daten liegen in der Cloud

Wir müssen Daten und Zugriff auch außerhalb unseres Netzwerkes schützen

Anforderungen CISO

Wie sicher – wie gefährdet – sind wir ?

Wie können wir die Gefährdung im Laufe der Zeit reduzieren ?

Wo sollen wir Prioritäten setzen ?

Wie stehen wir im Vergleich zu unserem Mitbewerbern ?

Die Gefahren sind real

TECH CYBERSECURITY

2

PROTOKOLL DES VERSAGENS

Das Handelsblatt veröffentlicht den

cked to send out fake

Panasonic bestätigt Zugriff durch Hacker, der monatelang bestand

Witold Pryjda am 30.11.2021 18:19 Uhr

prominen-

cker sich Zu-

EBAY

Rechner mit sensiblen Daten des Ausländeramtes verkauft

nderamtes

sowie Daten

nber ereignet

ns auf einige

Moritz Tremmel

17.05.2022, 06:48 Uhr

Nach Hackerangriff: Produktion bei Fendt läuft wieder

AKTUELLE BETRUGSWARNUNGEN

Cyberattacke auf deutsche Autoindustrie: Phishing-Mails

11. Mai 2022 um 13:29 Uhr

Gerrit Gerbig

Die deutsche Autoindustrie wird

Phishing-Mails dienen dabei zur

Werkstätten.

In Darmstadt, Mainz und Frankfurt

Hackerangriffe auf städtische Dienstleister – Folgen über mehrere Tage

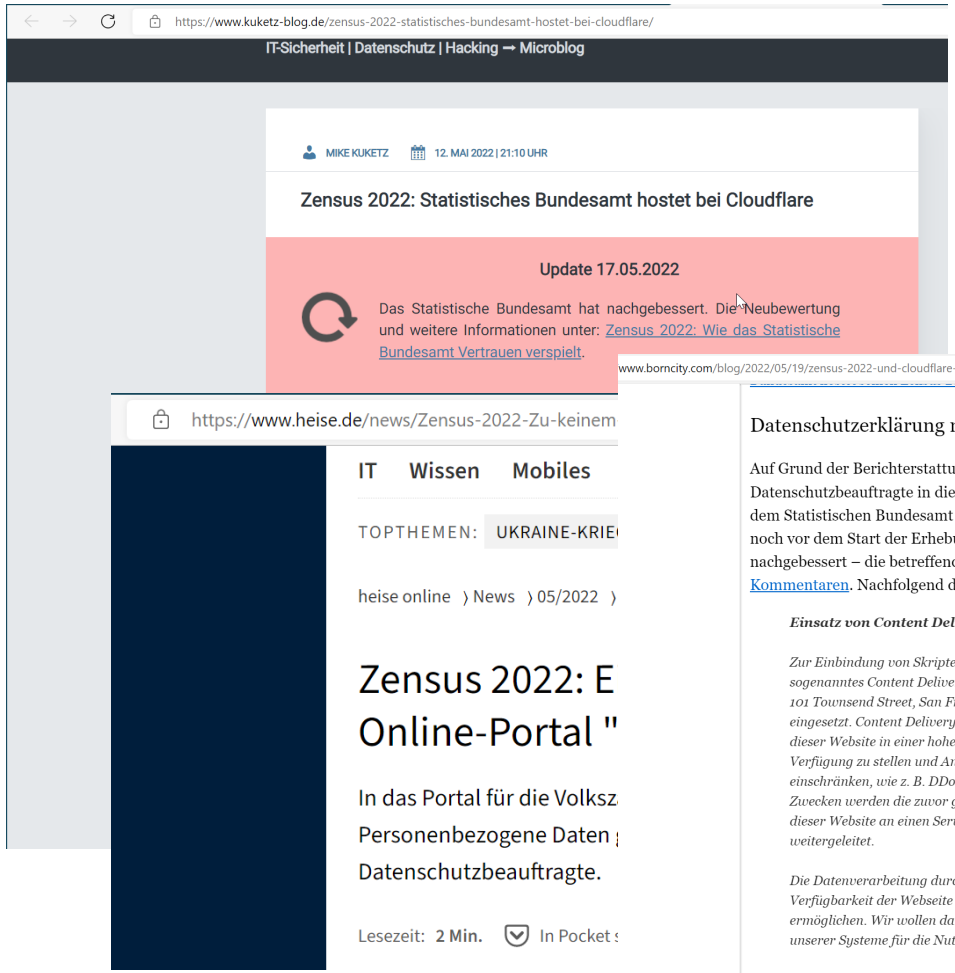
Von dpa, t-online, stn

Aktualisiert am 13.06.2022

Lesedauer: 2 Min.

Zensus 2022

zensus 2022



Zero Trust

Never Trust, Always Verify

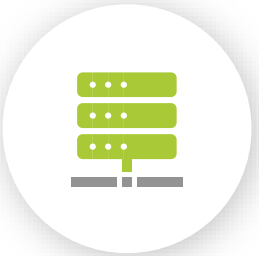
Ein moderner Sicherheitsansatz, bei dem jeder Zugriffsversuch so behandelt wird, als käme er aus einem nicht vertrauenswürdigen Netz

Zero Trust über den gesamten digitalen Bereich

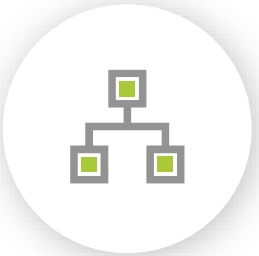
Identity

Endpoint Management

Apps



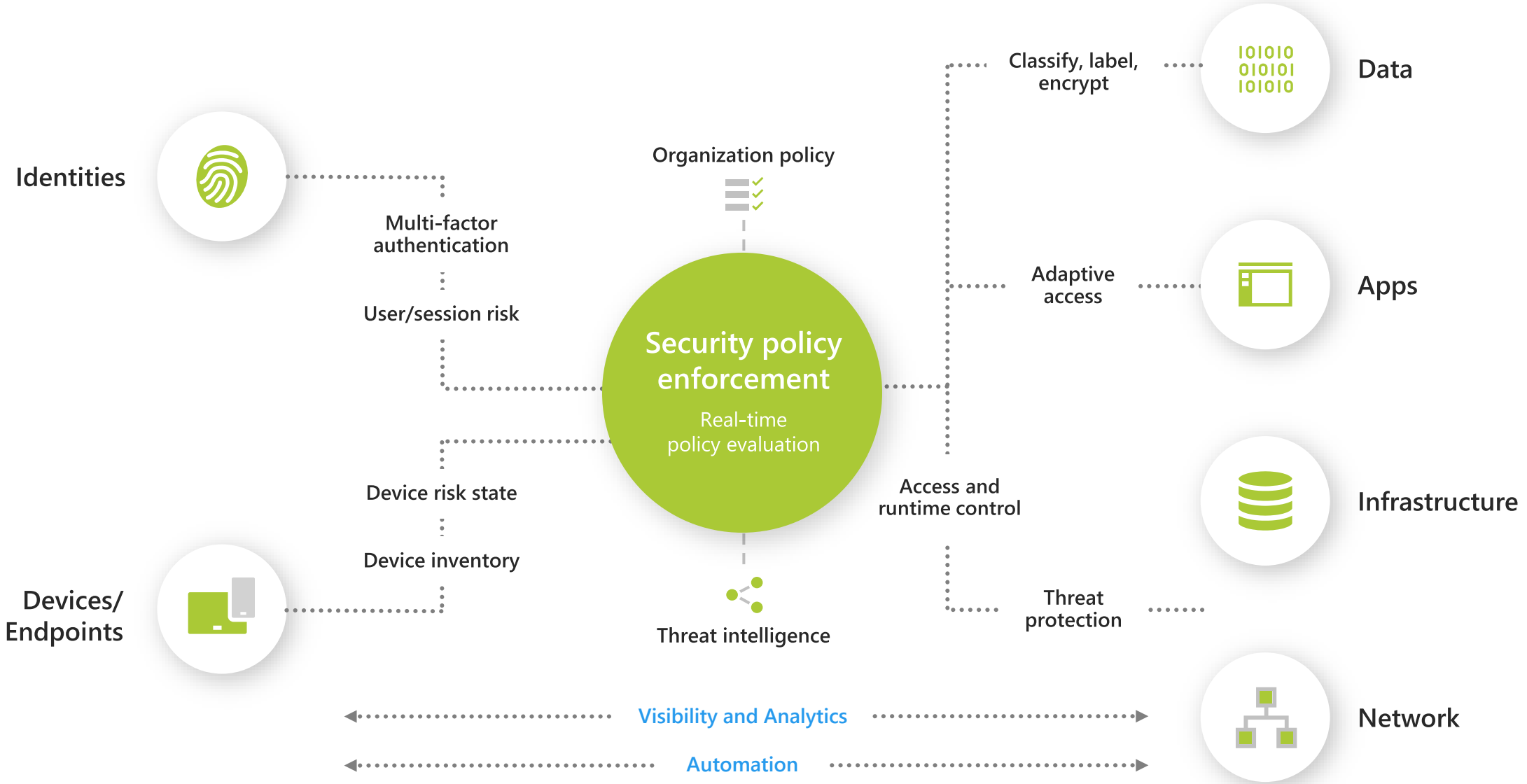
Infrastructure



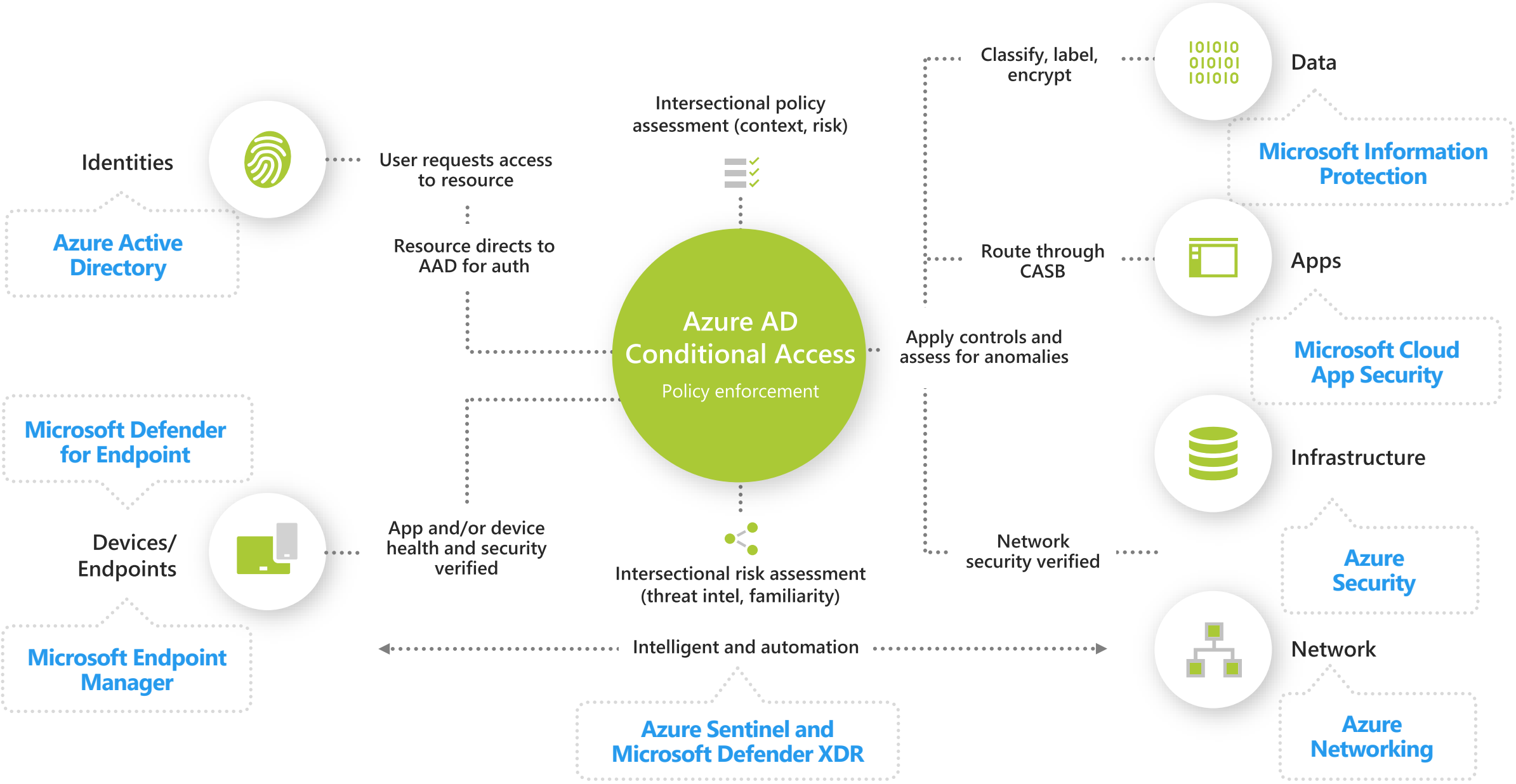
Networking

Data

Microsoft Zero Trust Architektur



Microsoft's Zero Trust Technologien



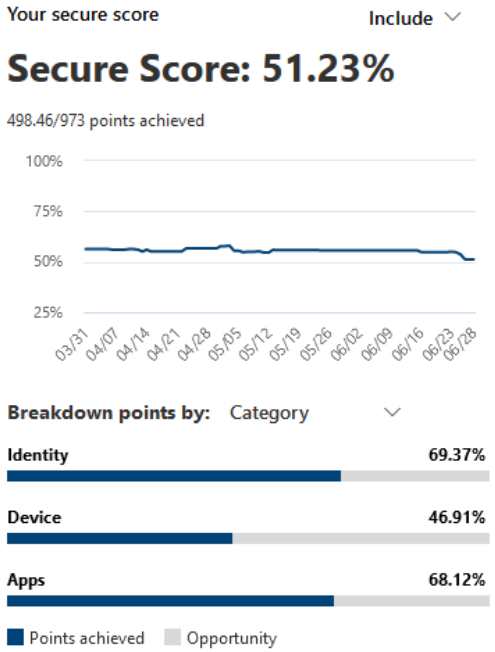
Dashboards – CISO

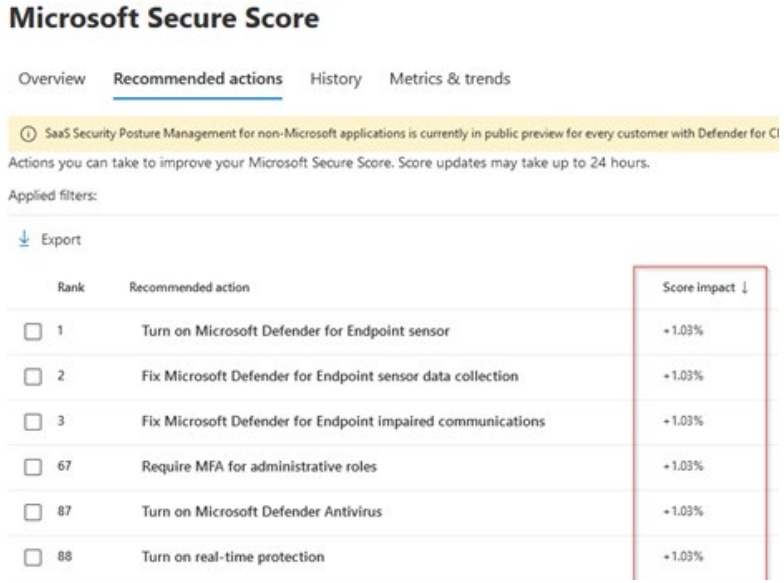
Wie sicher sind wir ?

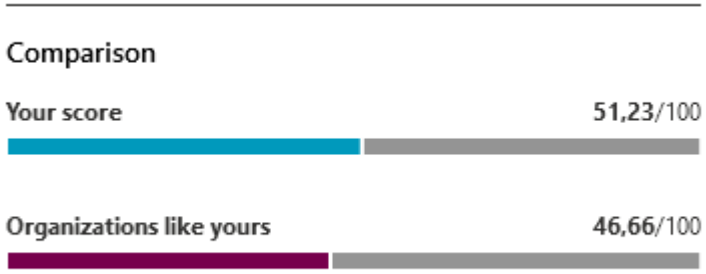
Was können wir zukünftig unsere Sicherheit verbessern ?

Wo sollen wir Prioritäten setzen ?

Wie sicher sind wir im Vergleich ?







Fragen/Anforderungen Admin

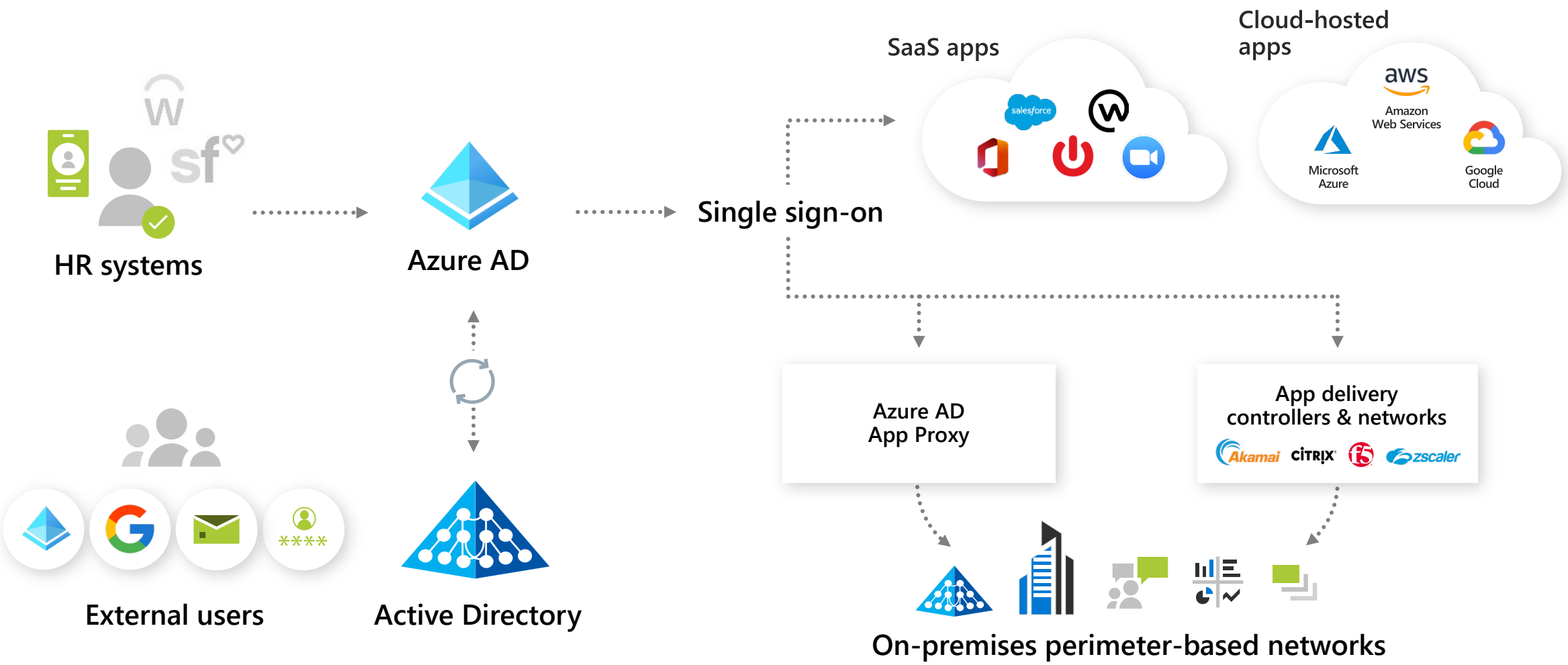
Wie können wir den Zugriff (Login) auf unsere Apps schützen ?

Zugriff von überall möglich – auch für Hacker

Wir benötigen eine Kontrolle der Zugriffe

Wir brauchen eine einfache Lösung

Sicherer Zugriff auf alle Anwendungen mit Single Sign On

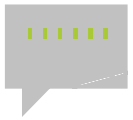


Einsatz der sichersten, brauchbarsten und kostengünstigsten Methoden

Bad: Password

Ukraine2022!
Sars-Cov-2
Covid-19
Maga2020!
123456
Qwertz
P@ssw0rd!
StopWar!22

Good: Password +



SMS

Voice

Better: Password +

Push Notification

Soft Tokens OTP

Hard Tokens OTP

Best: +

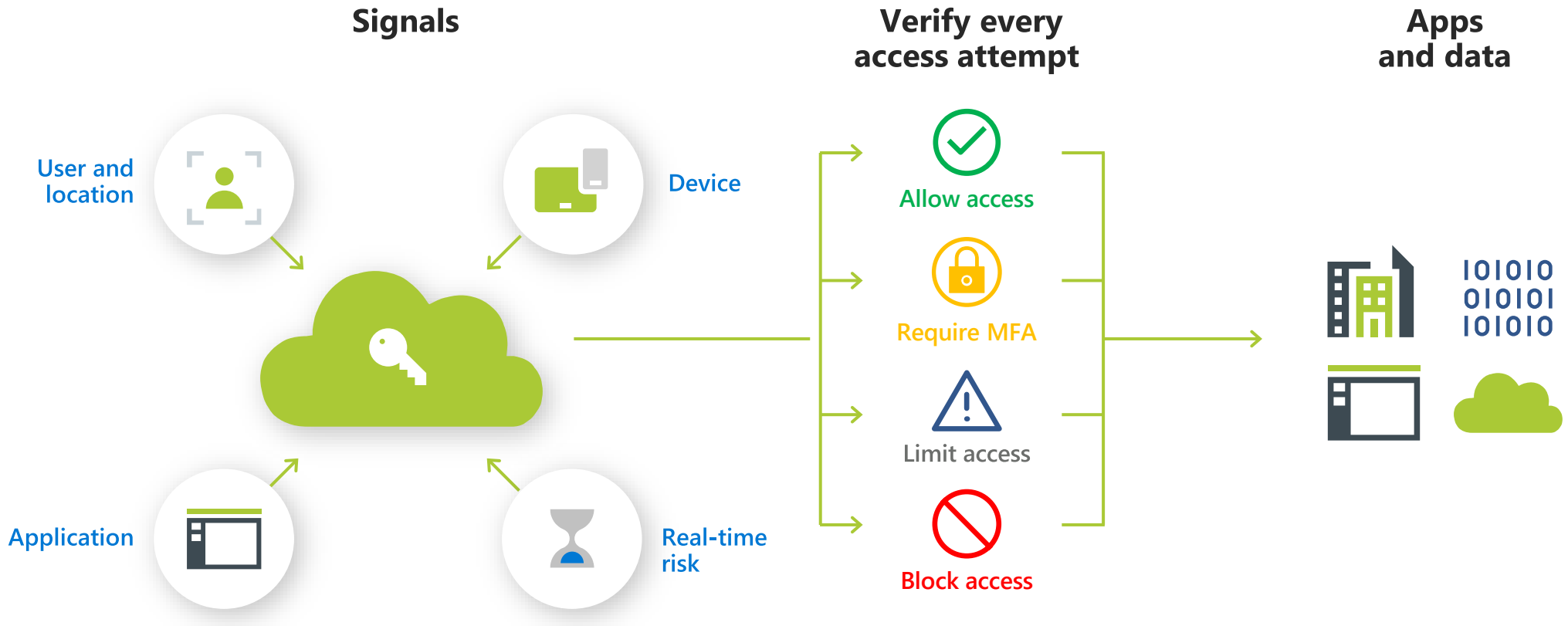
Microsoft Authenticator

Windows Hello

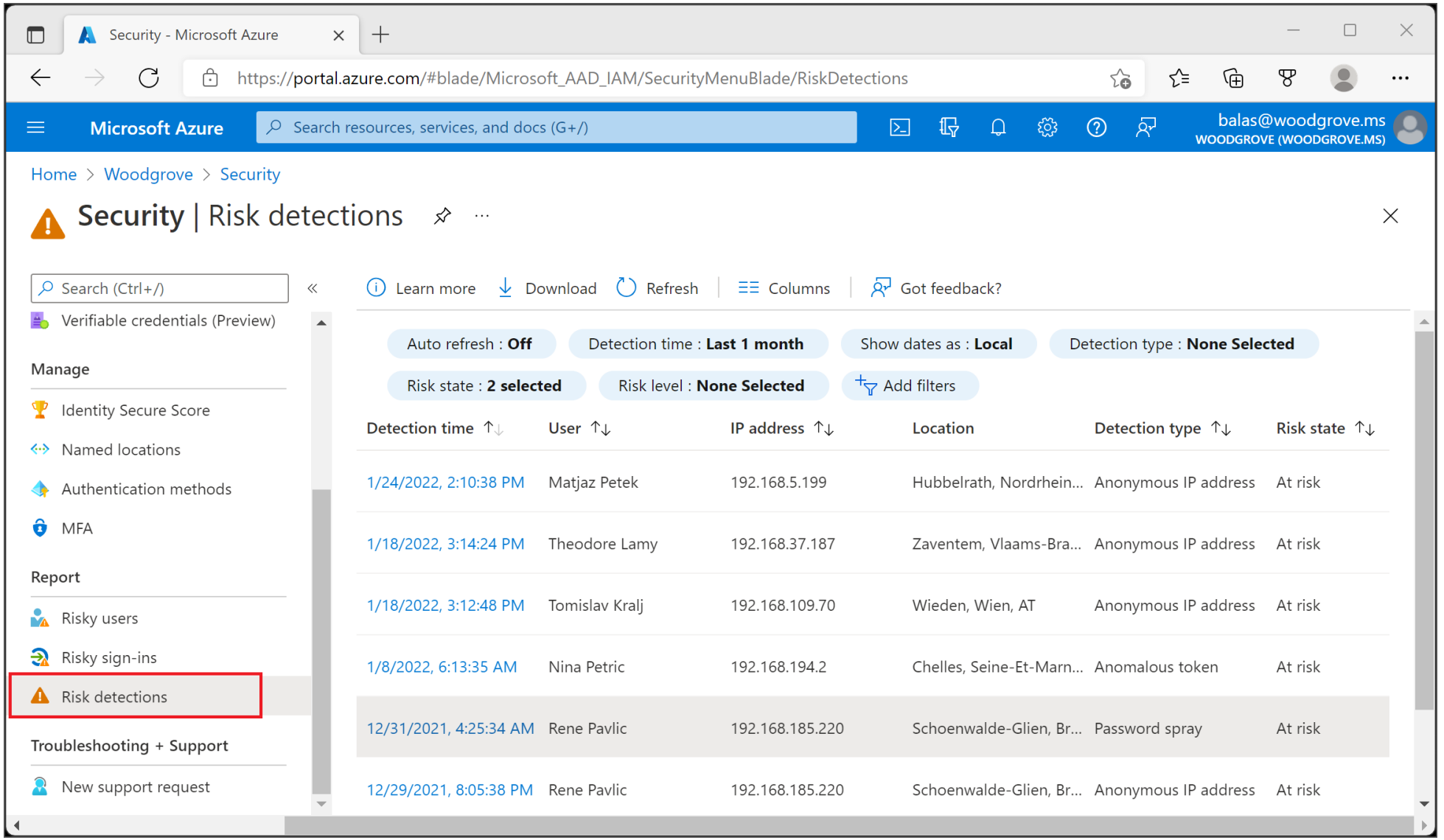
FIDO2 Security key

Multi-Faktor-Authentifizierung mit Conditional Access

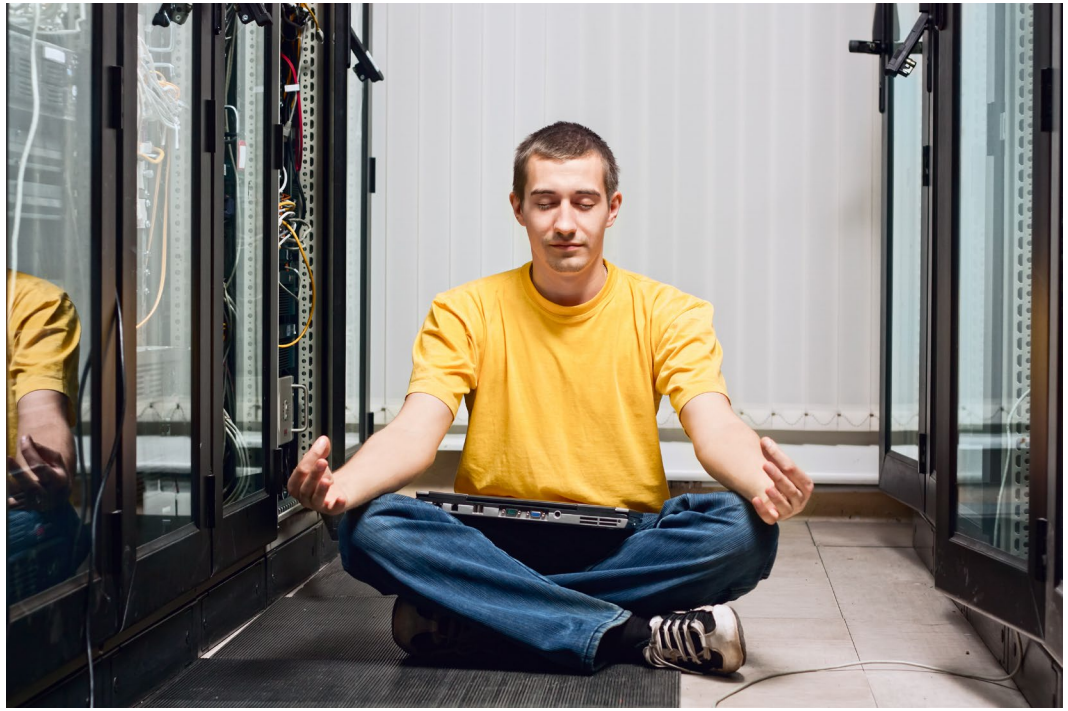
Durchsetzung strenger Schutzmaßnahmen und Risikobewertung bei der Gewährung von Zugang für Mitarbeiter und Partner



Logins überprüfen und riskante User erkennen



Fragen Admin



Wie können wir unsere Clients absichern, egal wo diese sich befinden ?

Windows Defender ist doch nur ein einfacher Virenscanner

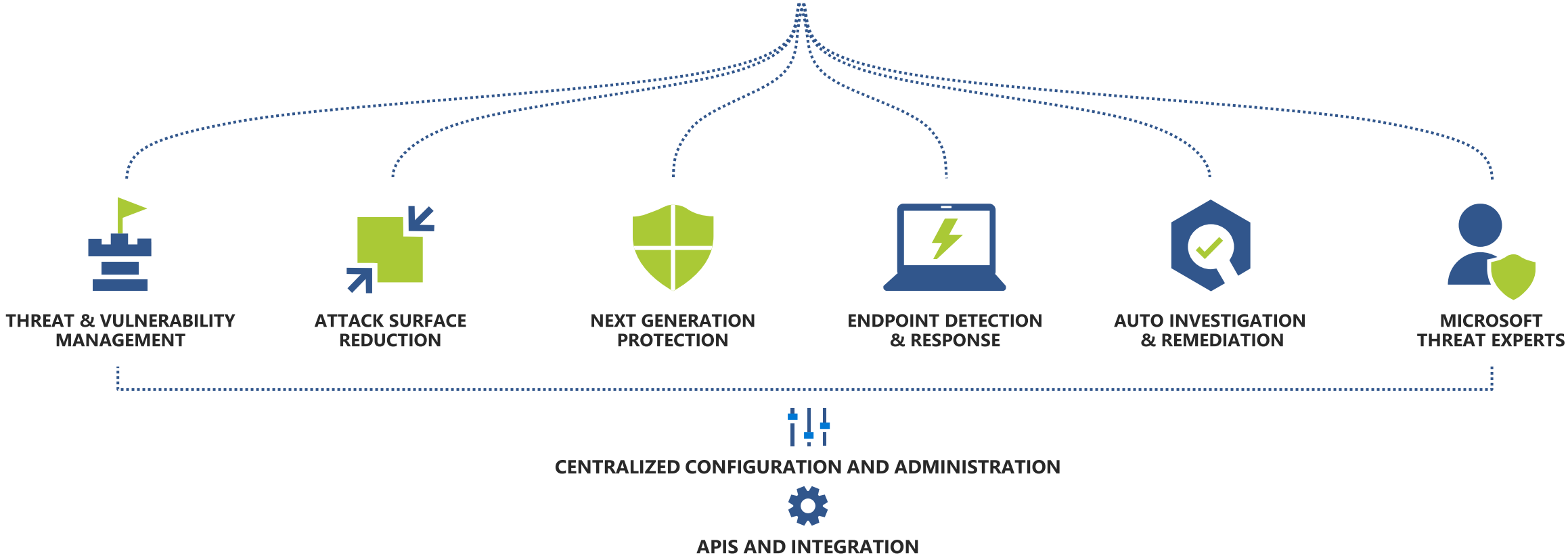
Kann man damit auch komplexe Angriffe abwehren ?

Kann ich sehen, ob ein Client eine Schwachstelle hat ?

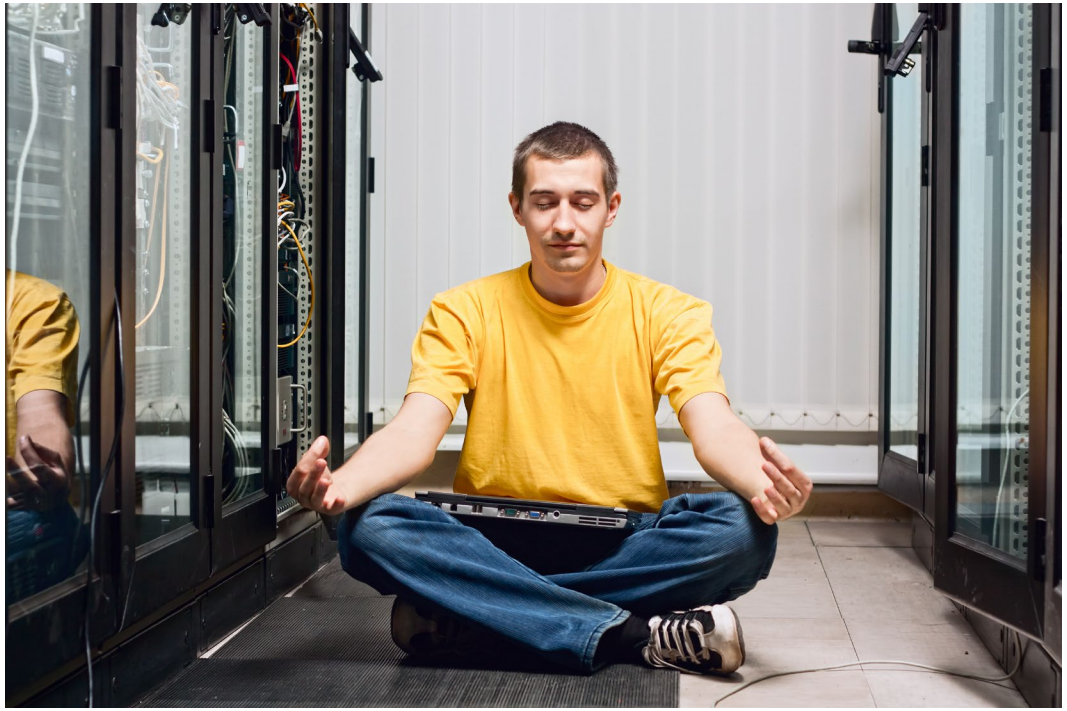
Was mache ich bei einem Vorfall ?

Microsoft Defender
for Endpoint

Threats are no match.



Fragen Admin



Wie können wir Daten und (Cloud)-Apps absichern ?

Welche Apps werden auf den Endgeräten benutzt ?

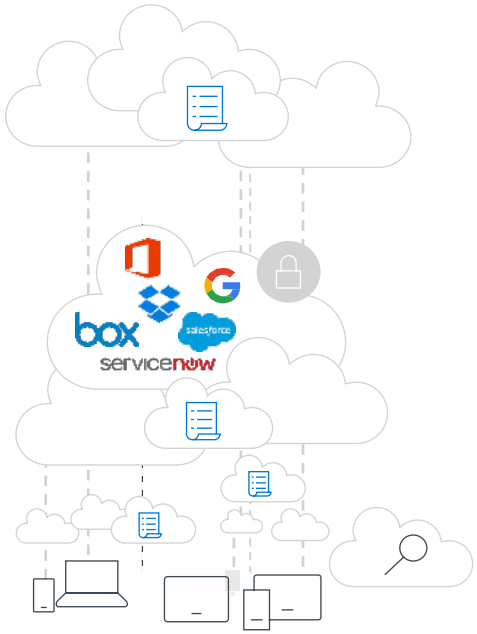
Haben wir evtl. eine Schatten-IT ?

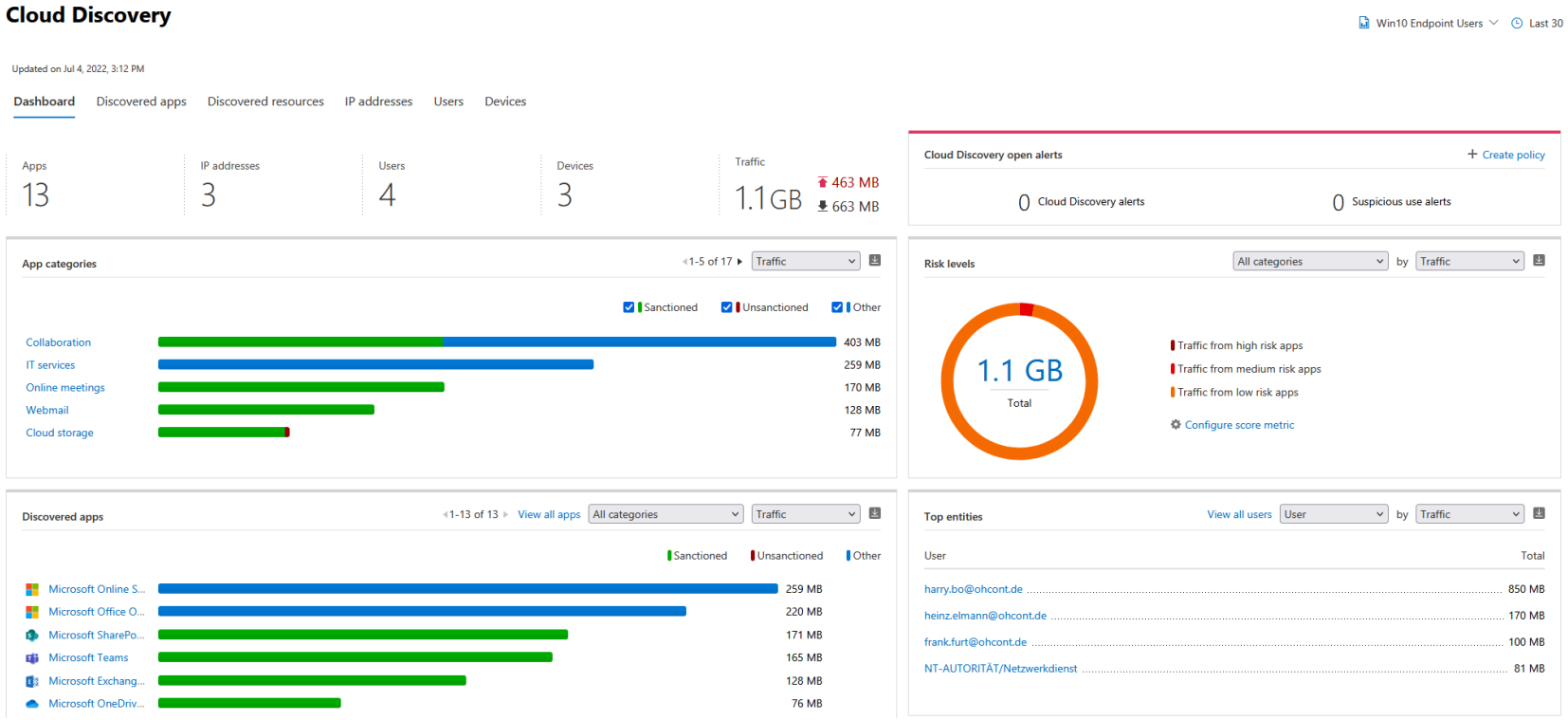
Wie können wir den Zugriff auf Daten steuern, z.B. mit Richtlinien ?

Wie weiß ich, ob die Benutzer Unternehmens-Richtlinien verletzen ?

Microsoft Defender for Cloud Apps

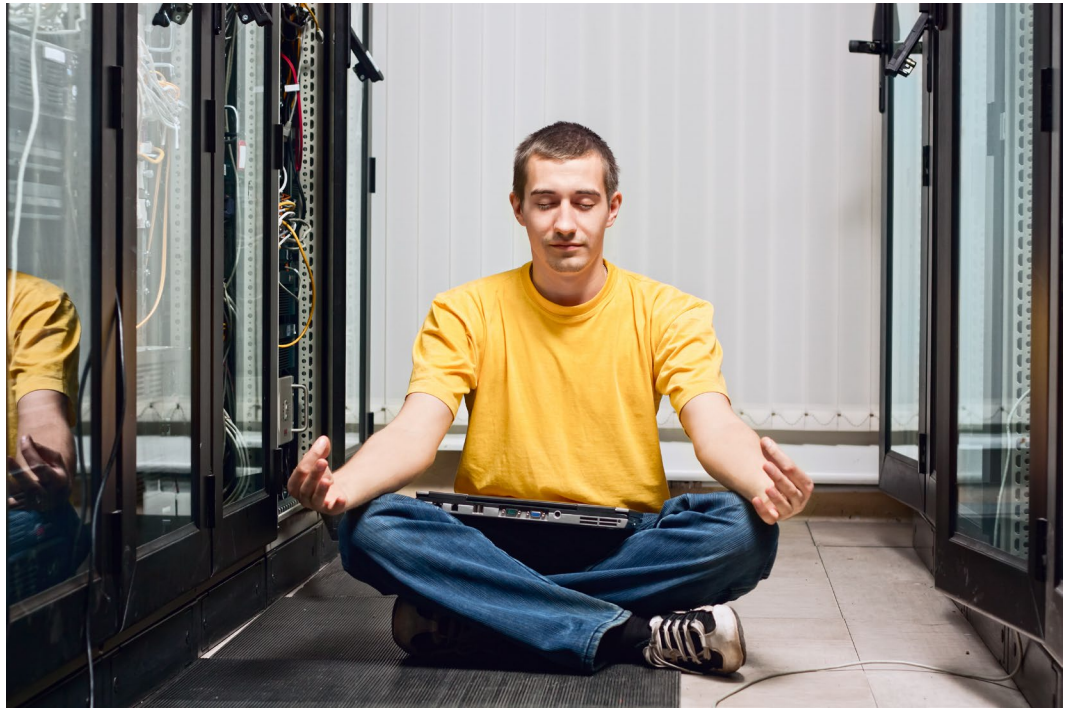
Eine umfassende, intelligente Sicherheitslösung, die die Transparenz, Echtzeitkontrolle und Sicherheit Ihres lokalen Netzwerks auf Ihre Cloud-Anwendungen ausweitet





Discover Control Protect

Fragen Admin



Wie können wir sensible Unternehmensdaten schützen ?

Es gibt Dokumente mit z.B. personenbezogenen Daten, die gelabelt werden sollten

Können sensible Daten automatisch in Dokumenten erkannt werden ?

Können auf Dokumente Rechte vergeben werden, die immer angewendet werden ?

Information Protection & Governance

Schutz und Verwaltung von Daten - wo auch immer sie gespeichert sind

Verstehen Sie Ihre Datenlandschaft und identifizieren Sie wichtige Daten in Ihrer hybriden Umgebung

Verhinderung der versehentlichen Weitergabe sensibler Informationen

Anwendung flexibler Schutzmaßnahmen wie Verschlüsselung, Zugangsbeschränkungen und visuelle Markierungen

Automatisches Aufbewahren, Löschen und Speichern von Daten und Aufzeichnungen in einer konformen Weise

Powered by an intelligent platform

Einheitlicher Ansatz für automatische Datenklassifizierung, Richtlinienverwaltung, Analysen und APIs

Cloud – Fragen CISO

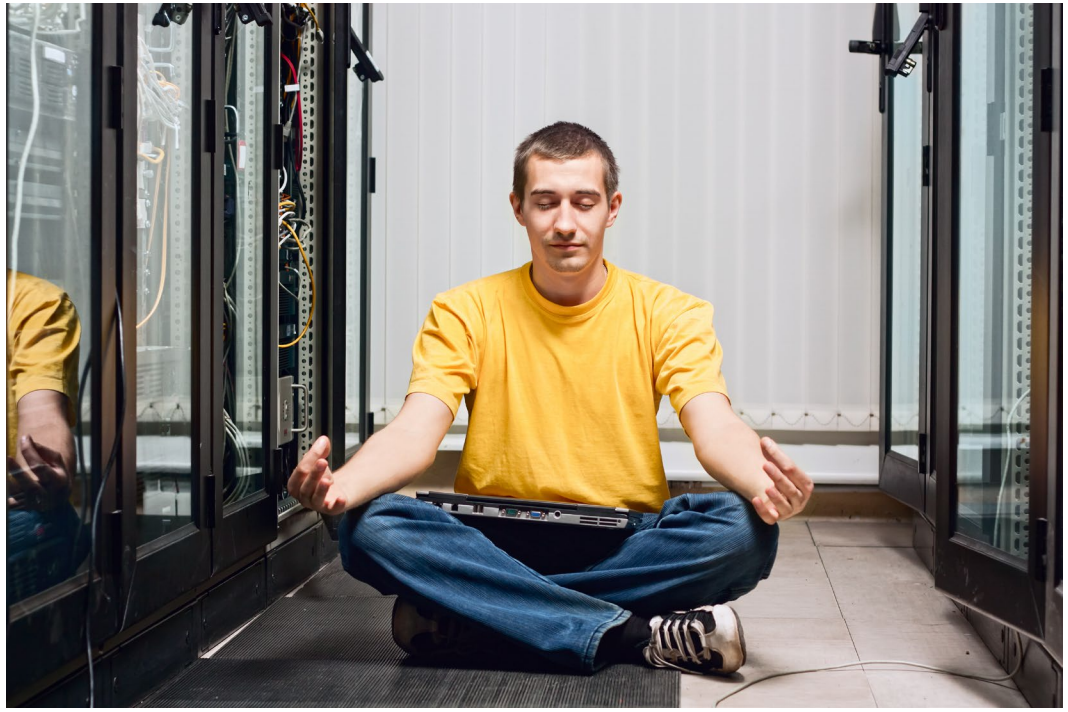
Wie sicher – wie gefährdet – sind wir ?

Wir möchten informiert werden, wenn Security-Incidents auftreten

Wir möchten automatisiert auf vordefinierte Incidents reagieren

Benötigen wir ein eigenes Team ?

Cloud – Fragen Admin



Wie können wir die Sicherheit überwachen ?

Es gibt sehr viele Dashboards …..

Gibt es eine zentrale Oberfläche wo alle Daten zusammengeführt werden ?

Können Angriffe oder Bedrohungen zentral nachverfolgt werden ?

Microsoft Sentinel

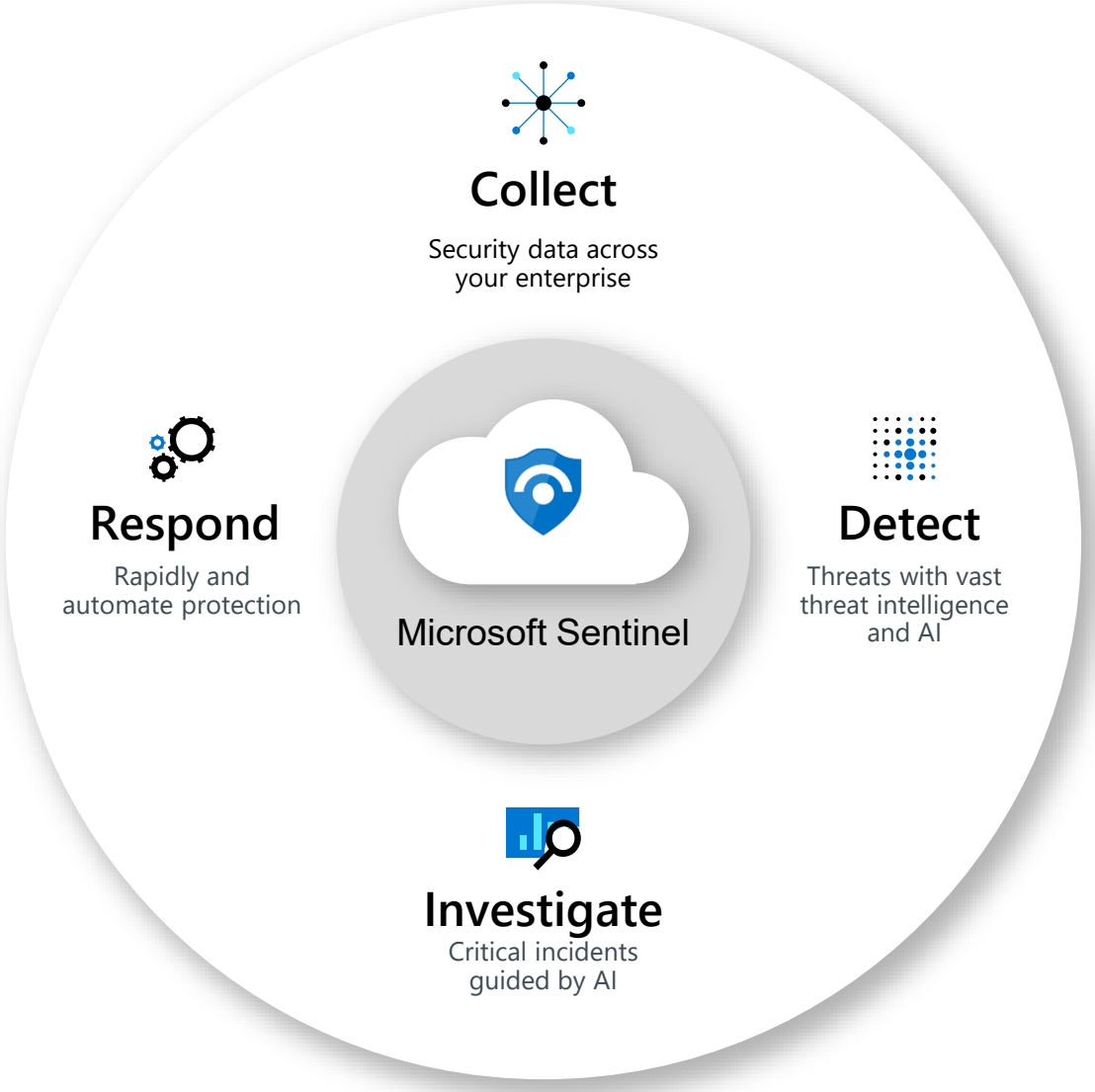
Cloud-natives SIEM für intelligente Sicherheitsanalysen für Ihr gesamtes Unternehmen

Unbegrenzte Geschwindigkeit und Skalierung der Cloud

Bringen Sie Ihre Office 365-Daten kostenlos mit

Einfache Integration mit Ihren bestehenden Tools

Schnellerer Schutz vor Bedrohungen mit KI an Ihrer Seite



Sammeln Sie Sicherheitsdaten auf Cloud-Ebene aus allen Quellen in Ihrem Unternehmen

Vorgefertigte Integration mit Microsoft-Lösungen

Konnektoren für viele Partnerlösungen (z.B. Google, AWS, usw.)

Unterstützung von Standard-Protokollformaten für alle Quellen

Zentrales Incidentmanagement

Daten und Fakten – darauf vertrauen

Sichern sie Ihre Daten und vertrauen sie nur auf Fakten

SWS und Microsoft liefern Ihnen Fakten

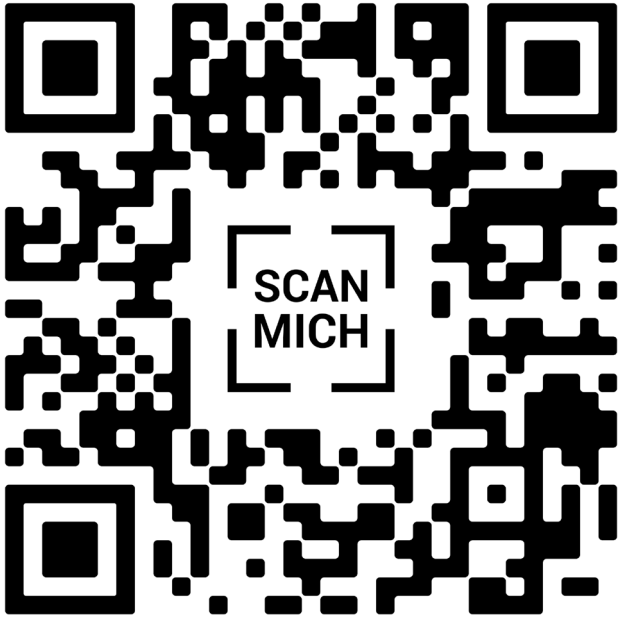
Wir liefern ihnen Lösungen für ihre Fragen

Wir zeigen ihnen auf wo sie handeln müssen

HANDELN SIE JETZT !

!! Brainshare Aktionsrabatt auf Microsoft Assessment-Workshops mit SWS !!

Anmelden unter: www.sws.de/microsoft-zero-trust



SWS COMPUTERSYSTEME
Member of ACP Group

BRAIN SHARE
SWS COMPUTERSYSTEME AG

Vielen Dank für eure Aufmerksamkeit.

Fragen?

IT for innovators.

Member of ACP Group