



Microsoft Zero Trust

Vertrauen Sie nur auf Fakten und
schützen sie Ihre Daten



Oliver Hien

Senior Consultant Datacenter

Microsoft Security, Messaging



Andreas Wach

Cloud Solution Architect

Security, Compliance & Identity





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



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



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

PROTOKOLL DES VERSAGENS

Das Handelsblatt veröffentlicht den **acked to send out fake**

2

Panasonic bestätigt Zugriff durch Hacker, der monatelang bestand

Witold Pryjda am 30.11.2021 18:19 Uhr

EBAY

Rechner mit sensiblen Daten des Ausländeramtes verkauft

prominen-
cker sich Zu-

Ein a
De
be
ha
Da

17.05.2022, 06:48 Uhr

Nach Hackerangriff: Produktion bei Fendt läuft wieder

nderamtes

sowie Daten
ber ereignet
ns auf einige



Seit Montag
das Unterne
Ermittlung

AKTUELLE BETRUGSWARNUNGEN

Moritz Tremmel

Cyberattacke auf deutsche Autoindustrie: Phishing-Mails

Von

Nach zehn T
Traktorenhe
habe das Ur
teilte Fendt
Cyberattack
elf Tage nac
noch nicht e

11. Mai 2022 um 13:29 Uhr
Gerrit Gerbig

Weltweit
Der US-ame
Bemühunge
Ein Großteil

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.





© Statistische Ämter des Bundes und der Länder

IT-Sicherheit | Datenschutz | Hacking → Microblog

MIKE KUKETZ 12. MAI 2022 | 21:10 UHR

Zensus 2022: Statistisches Bundesamt hostet bei Cloudflare

Update 17.05.2022

Das Statistische Bundesamt hat nachgebessert. Die Neubewertung und weitere Informationen unter: [Zensus 2022: Wie das Statistische Bundesamt Vertrauen verspielt.](#)

https://www.heise.de/news/Zensus-2022-Zu-keinem

IT Wissen Mobiles

TOPTHEMEN: UKRAINE-KRIE

heise online } News } 05/2022 }

Zensus 2022: E Online-Portal "

In das Portal für die Volksz Personenbezogene Daten ; Datenschutzbeauftragte.

Lesezeit: 2 Min. In Pocket :

Datenschutzerklärung nachgebessert

Auf Grund der Berichterstattung hatte sich Herr Kelber als Datenschutzbeauftragte in die Diskussion eingeschaltet und Klärungen mit dem Statistischen Bundesamt durchgeführt. Samstag, den 14. Mai 2022, also noch vor dem Start der Erhebung, wurde die Datenschutzerklärung nachgebessert – die betreffende Diskussion/Information findet sich in [diesen Kommentaren](#). Nachfolgend der betreffende Passus, der ergänzt wurde.

Einsatz von Content Delivery Network

Zur Einbindung von Skripten und Bibliotheken auf dieser Webseite wird ein sogenanntes Content Delivery Network (CDN) der Firma Cloudflare, Inc., 101 Townsend Street, San Francisco, California 94107, USA ("Cloudflare") eingesetzt. Content Delivery Networks haben den Zweck, Ihnen die Inhalte dieser Website in einer hohen Verfügbarkeit und Geschwindigkeit zur Verfügung zu stellen und Angriffe auf die Webseite, die die Verfügbarkeit einschränken, wie z. B. DDoS -Angriffe, besser abzuwehren. Zu diesen Zwecken werden die zuvor genannten Zugriffsdaten bei jeder Nutzung dieser Website an einen Server innerhalb der EU der o.g. Firma weitergeleitet.

Die Datenverarbeitung durch Cloudflare ist erforderlich, um die hohe Verfügbarkeit der Webseite auch in unsicheren Zeiten im Internet zu ermöglichen. Wir wollen damit eine hohe Funktionsfähigkeit und Sicherheit unserer Systeme für die Nutzer gewährleisten.

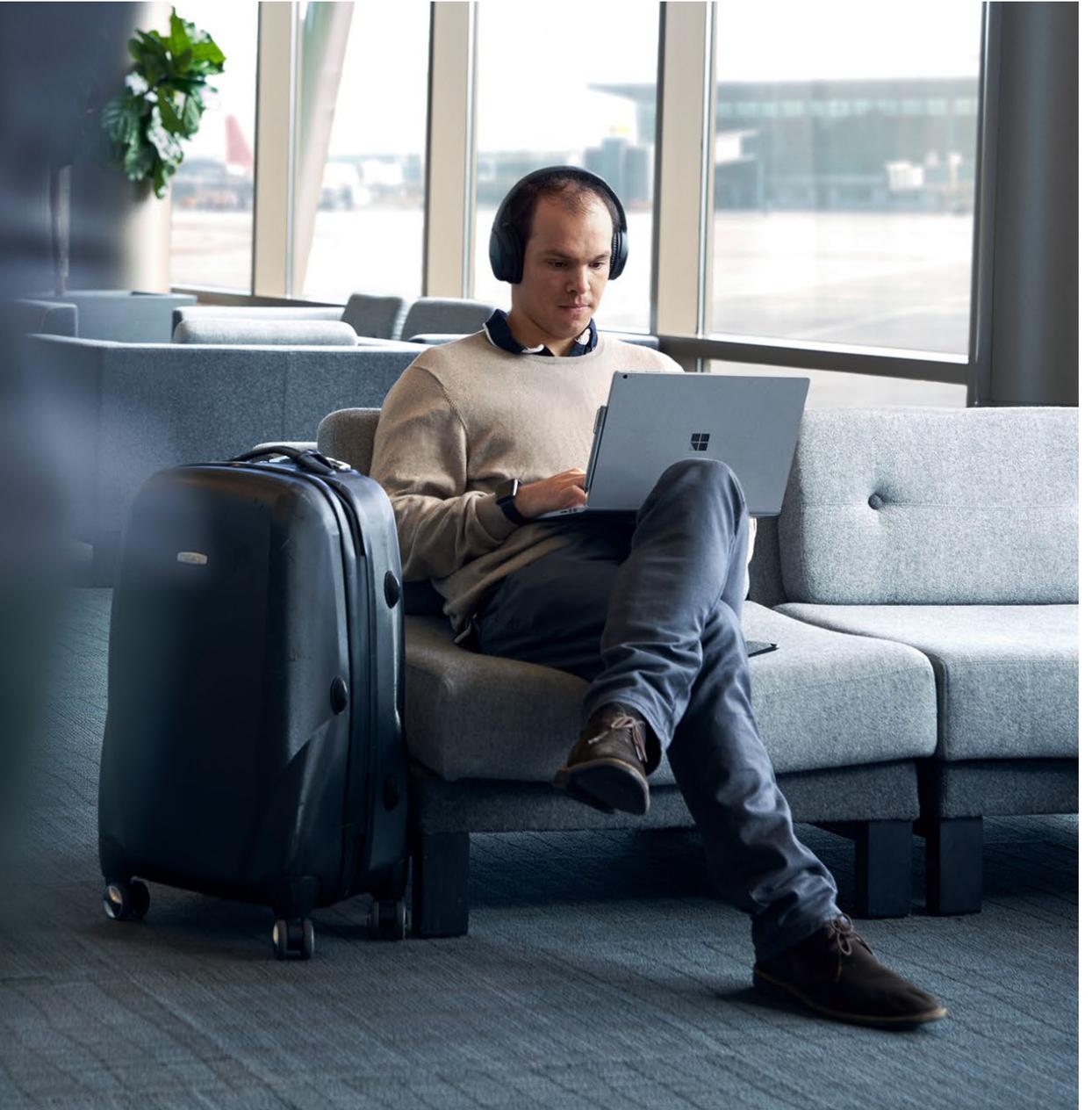
In diesem Zusammenhang weisen wir daraufhin, dass unter Umständen die genannten Daten von Cloudflare in einen Drittstaat (insbesondere USA) transferiert werden können, wenn dies zur Einhaltung eines Gesetzes oder aufgrund einer verbindlichen Anordnung einer Regierungsbehörde in den USA erforderlich ist.

Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. e) DS-GVO in Verbindung mit § 3 BDSG in Verbindung mit den Zensusgesetzen in Verbindung mit den Standarddatenschutzklauseln nach Art. 46 Abs. 2 c) DS-GVO sowie weiterer im Vertrag mit der Firma Cloudflare gesicherten Garantien. Weitere Informationen zur Datenverarbeitung seitens der Firma Cloudflare finden Sie in der „[Cloudflare Privacy Policy](#)“.

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



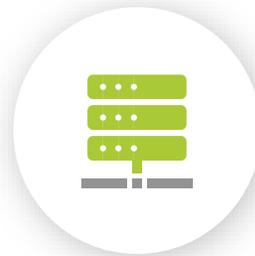
Identity



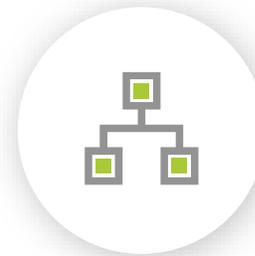
Endpoint
Management



Apps



Infrastructure

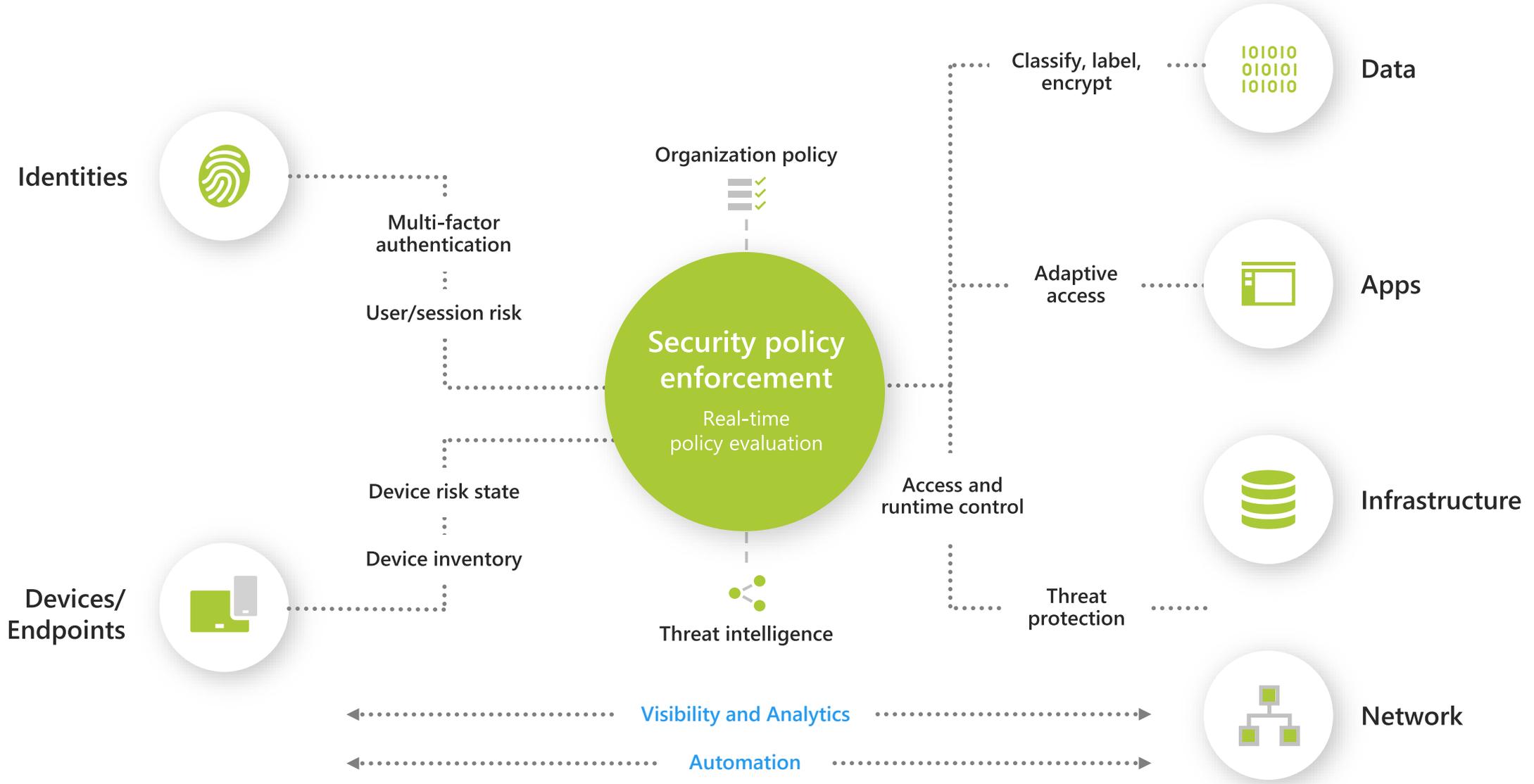


Networking

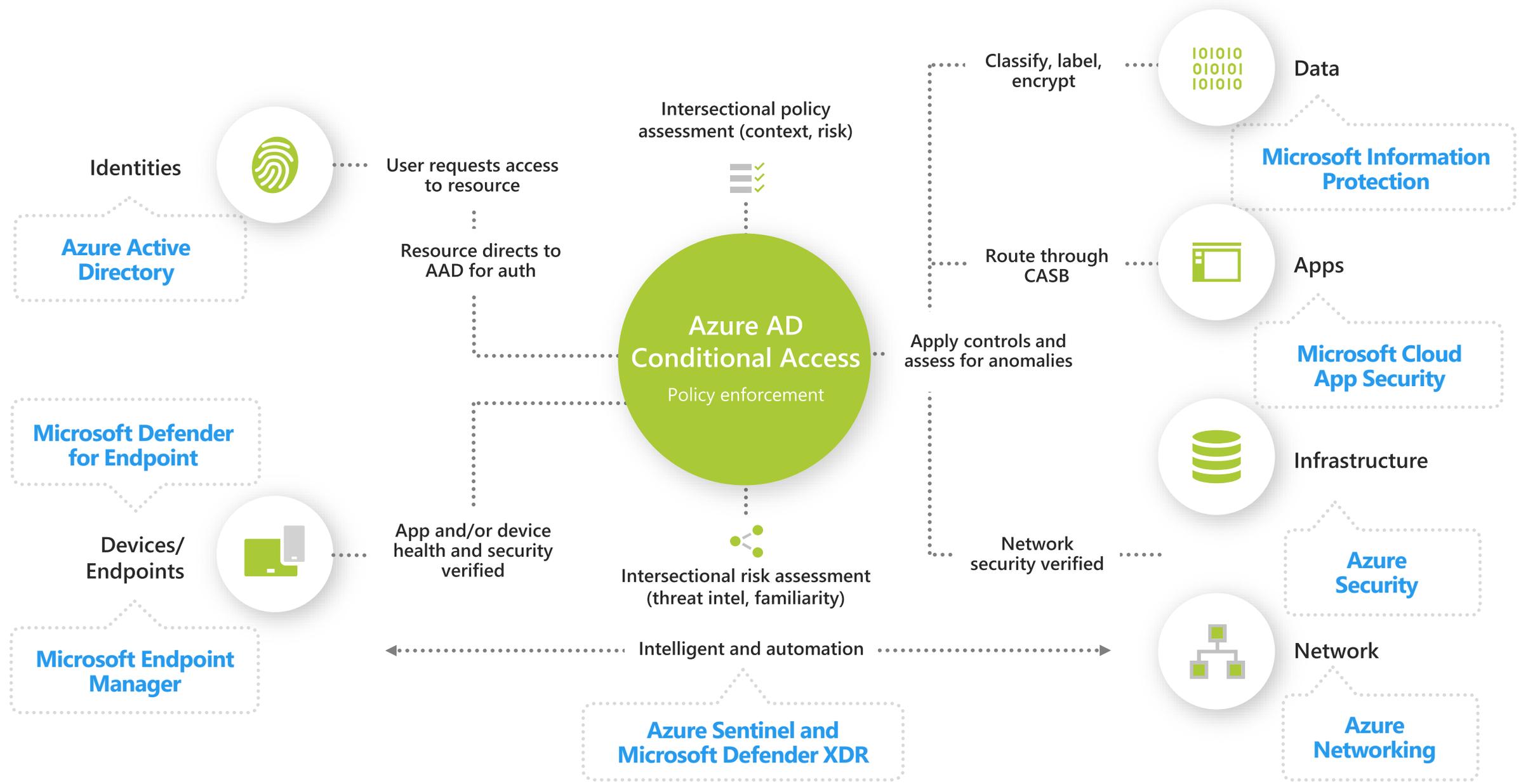


Data

Microsoft Zero Trust Architektur



Microsoft's Zero Trust Technologien



Wie sicher sind wir ?

Was können wir
zukünftig unsere
Sicherheit verbessern ?

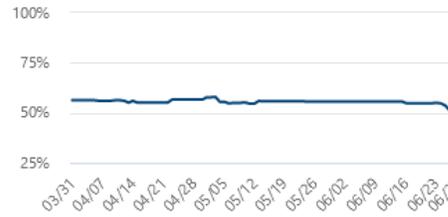
Wo sollen wir
Prioritäten setzen ?

Wie sicher sind wir im
Vergleich ?

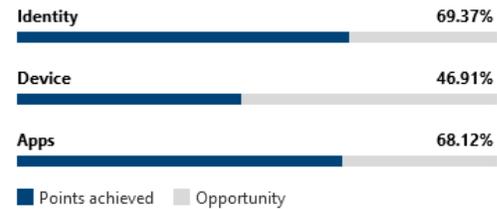
Your secure score Include ▾

Secure Score: 51.23%

498,46/973 points achieved



Breakdown points by: Category ▾



Microsoft Secure Score

Overview Recommended actions History Metrics & trends

SaaS Security Posture Management for non-Microsoft applications is currently in public preview for every customer with Defender for Cloud.

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Applied filters:

Export

Rank	Recommended action	Score impact ↓
<input type="checkbox"/> 1	Turn on Microsoft Defender for Endpoint sensor	+1.03%
<input type="checkbox"/> 2	Fix Microsoft Defender for Endpoint sensor data collection	+1.03%
<input type="checkbox"/> 3	Fix Microsoft Defender for Endpoint impaired communications	+1.03%
<input type="checkbox"/> 67	Require MFA for administrative roles	+1.03%
<input type="checkbox"/> 87	Turn on Microsoft Defender Antivirus	+1.03%
<input type="checkbox"/> 88	Turn on real-time protection	+1.03%

Comparison

Your score 51,23/100



Organizations like yours 46,66/100





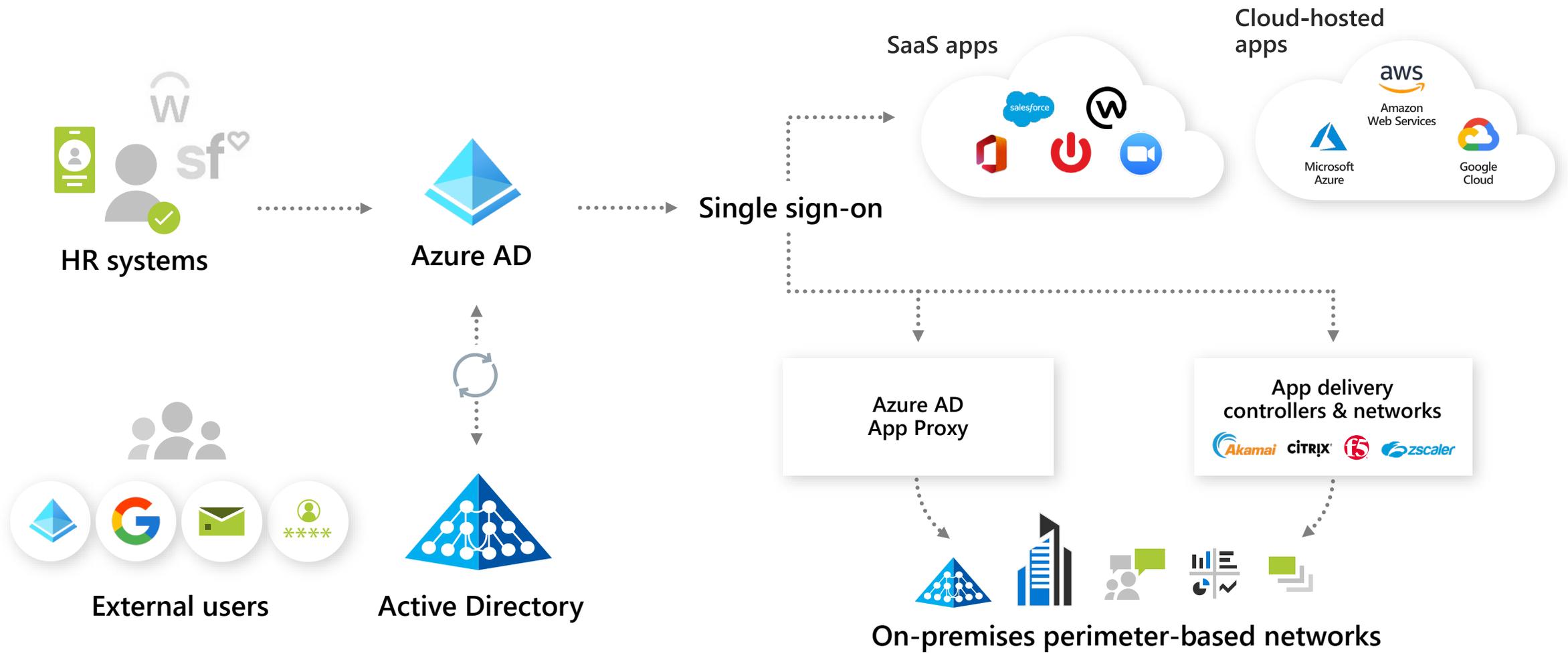
Wie können wir den Zugriff (Login) auf unsere Apps schützen ?

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



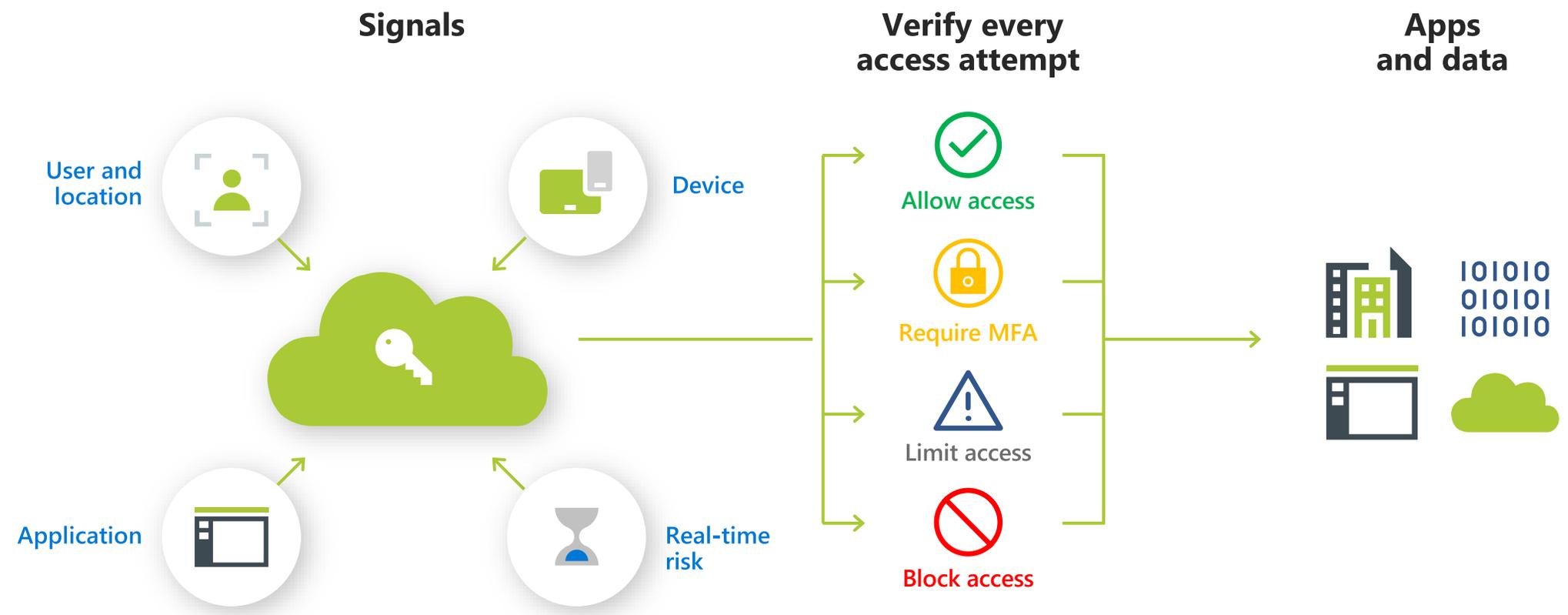
Windows
Hello



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

Microsoft Azure Security - Microsoft Azure

https://portal.azure.com/#blade/Microsoft_AAD_IAM/SecurityMenuBlade/RiskDetections

Microsoft Azure Search resources, services, and docs (G+)

Home > Woodgrove > Security

Security | Risk detections

Search (Ctrl+/) << Learn more Download Refresh Columns Got feedback?

Auto refresh : **Off** Detection time : **Last 1 month** Show dates as : **Local** Detection type : **None Selected**

Risk state : **2 selected** Risk level : **None Selected** Add filters

Detection time ↑↓	User ↑↓	IP address ↑↓	Location	Detection type ↑↓	Risk state ↑↓
1/24/2022, 2:10:38 PM	Matjaz Petek	192.168.5.199	Hubbelrath, Nordrhein...	Anonymous IP address	At risk
1/18/2022, 3:14:24 PM	Theodore Lamy	192.168.37.187	Zaventem, Vlaams-Bra...	Anonymous IP address	At risk
1/18/2022, 3:12:48 PM	Tomislav Kralj	192.168.109.70	Wieden, Wien, AT	Anonymous IP address	At risk
1/8/2022, 6:13:35 AM	Nina Petric	192.168.194.2	Chelles, Seine-Et-Marn...	Anomalous token	At risk
12/31/2021, 4:25:34 AM	Rene Pavlic	192.168.185.220	Schoenwalde-Glien, Br...	Password spray	At risk
12/29/2021, 8:05:38 PM	Rene Pavlic	192.168.185.220	Schoenwalde-Glien, Br...	Anonymous IP address	At risk

Manage

- Verifiable credentials (Preview)

Report

- Risky users
- Risky sign-ins
- Risk detections**

Troubleshooting + Support

- New support request



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

Windows Defender ist doch nur ein einfacher Virens Scanner

Kann man damit auch komplexe Angriffe abwehren ?

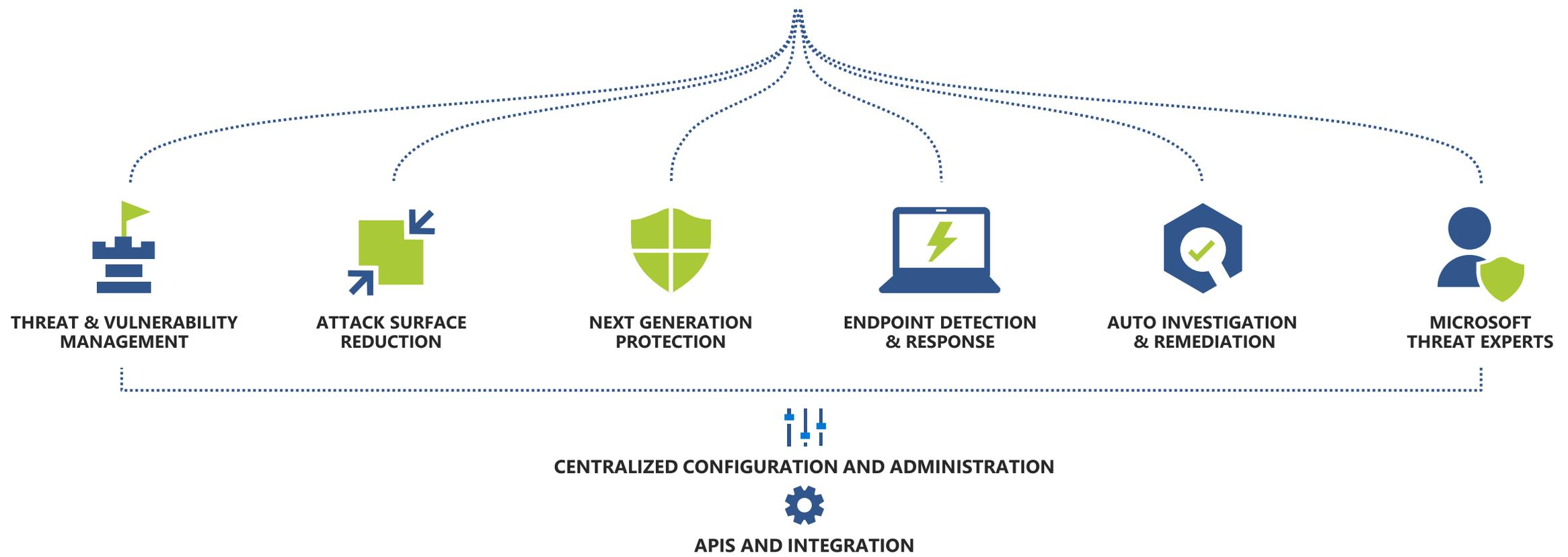
Kann ich sehen, ob ein Client eine Schwachstelle hat ?

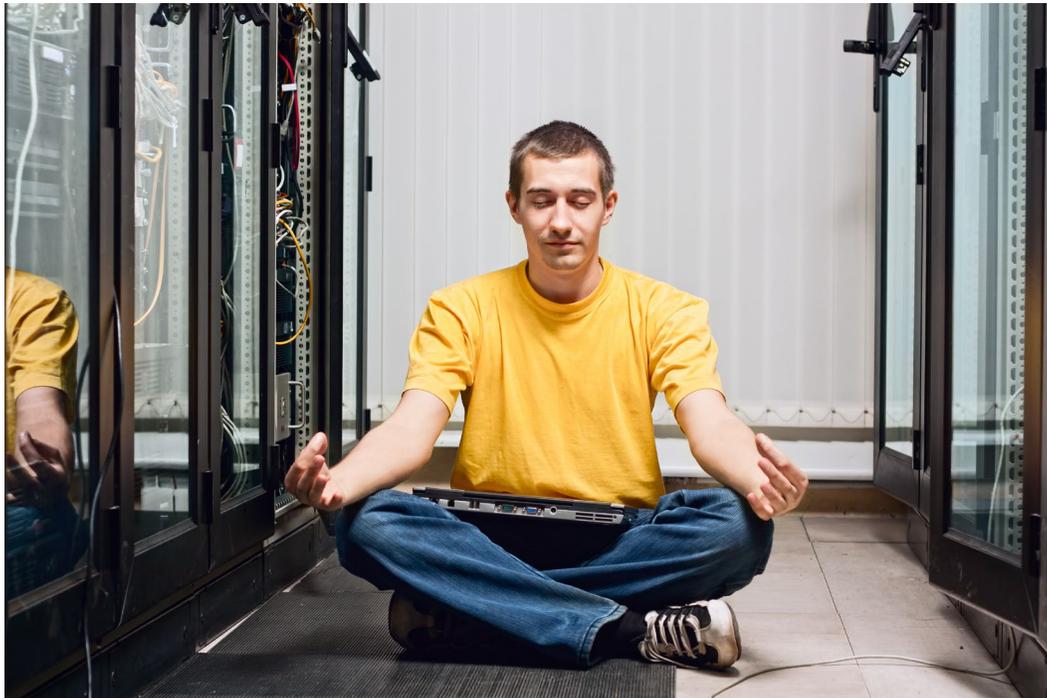
Was mache ich bei einem Vorfall ?



Microsoft Defender for Endpoint

Threats are no match.





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

Welche Apps werden auf den Endgeräten benutzt ?

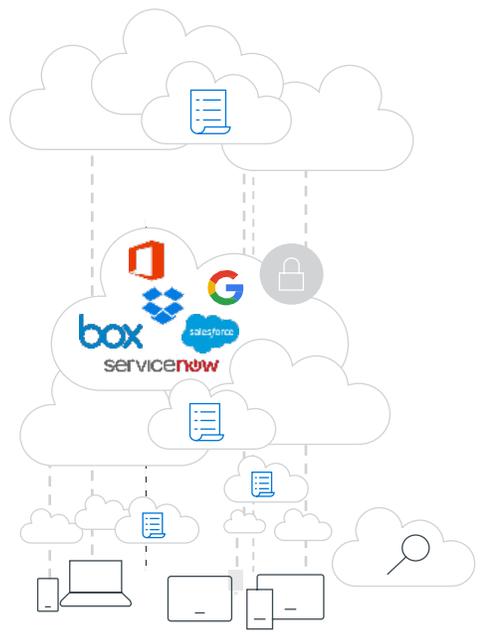
Haben wir evtl. eine Schatten-IT ?

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



Cloud Discovery

Updated on Jul 4, 2022, 3:12 PM

Win10 Endpoint Users | Last 30

Dashboard | Discovered apps | Discovered resources | IP addresses | Users | Devices

Apps: 13 | IP addresses: 3 | Users: 4 | Devices: 3 | Traffic: 1.1 GB (463 MB ↑, 663 MB ↓)

Cloud Discovery open alerts: 0 Cloud Discovery alerts, 0 Suspicious use alerts

Risk levels: 1.1 GB Total

Top entities: User

App categories	Sanctioned	Unsanctioned	Other	Total
Collaboration	~350 MB	~50 MB	~0 MB	403 MB
IT services	~200 MB	~50 MB	~0 MB	259 MB
Online meetings	~150 MB	~20 MB	~0 MB	170 MB
Webmail	~120 MB	~0 MB	~0 MB	128 MB
Cloud storage	~70 MB	~0 MB	~0 MB	77 MB

Discovered apps	Sanctioned	Unsanctioned	Other	Total
Microsoft Online S...	~200 MB	~50 MB	~0 MB	259 MB
Microsoft Office O...	~150 MB	~70 MB	~0 MB	220 MB
Microsoft SharePo...	~150 MB	~20 MB	~0 MB	171 MB
Microsoft Teams	~140 MB	~25 MB	~0 MB	165 MB
Microsoft Exchang...	~120 MB	~0 MB	~0 MB	128 MB
Microsoft OneDriv...	~70 MB	~0 MB	~0 MB	76 MB

User	Total
harry.bo@ohcont.de	850 MB
heinz.elmann@ohcont.de	170 MB
frank.furt@ohcont.de	100 MB
NT-AUTORITÄT/Netzwerkdiens...	81 MB

Discover

Control

Protect



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 ?

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



Powered by an intelligent platform

Einheitlicher Ansatz für automatische Datenklassifizierung, Richtlinienverwaltung, Analysen und APIs



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 ?



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





**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





**Vielen Dank für eure
Aufmerksamkeit.**

Fragen?

**IT for
innovators.**

Member of ACP Group