Microsoft 365 Defender

Thomas Schottenheim
Business Development Manager Microsoft Security

ARROW

tagesschau

Sendung verpasst?

Startseite ▸ Inland ▸ Gesellschaft ▸ Hunderte Unternehmen in Deutschland von Hac

Hunderte Unternehmen betroffen

Globale Hackerwelle trifft Deutschland

Stand: 06.02.2023 14:27 Uhr

Eine globale Welle von Cyberangriffen hat auch deutsche Unternehmen und Institutionen lahmgelegt. Laut dem zuständigen Bundesamt könnten Hunderte Firmen betroffen sein. Eine Software-Aktualisierung könne die Sicherheitslücke schließen.

Bei einer groß angelegten globalen Cyberangriffswelle mit Erpressungssoftware sind auch Firmen und öffentliche Einrichtungen in Deutschland geschädigt worden. "Nach aktuellem Kenntnisstand scheint es

Wirtschaftsunternehmen in Deutschland stehen im Fokus von Cyberkriminellen weltweit. Ihr Ziel ist es, Daten, Informationen und Know-How deutscher Firmen zu stehlen oder diese, beispielsweise mittels der Androhung oder Durchführung von DDoS-Attacken, digital zu erpressen. Dies trifft nicht nur auf große international tätige Konzerne zu, sondern auch auf national tätige Unternehmen des Mittelstandes. Aber auch unspezifische, breit gestreute Angriffe, wie beispielweise durch Ransomware, stellen eine hohe Gefahr für die IT-Infrastrukturen von Unternehmen aller Größen dar.

Quelle: Bundeskriminalamt

»Deutschlandweite Kampagne«

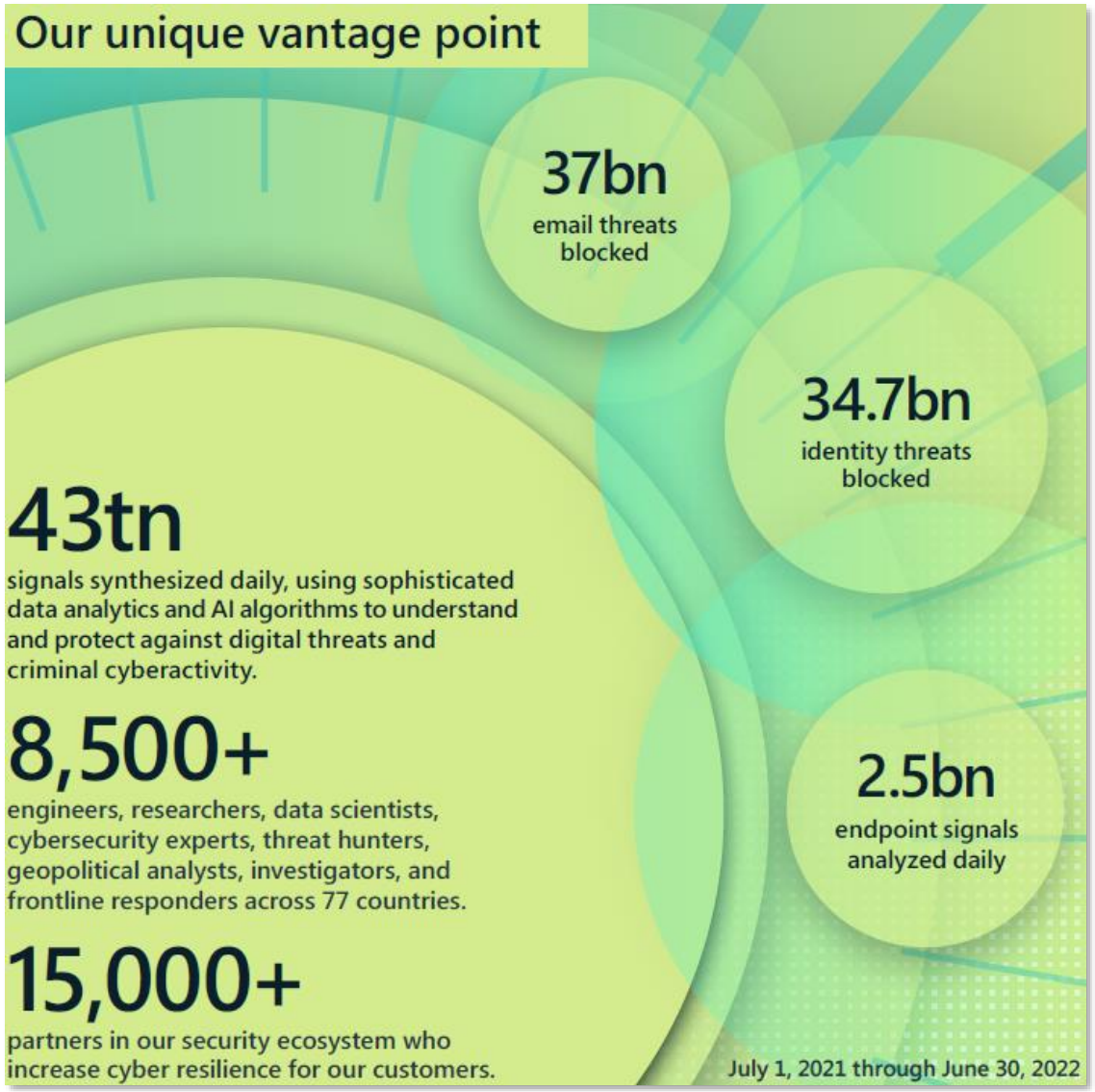
Cyberattacken auf mehrere deutsche Ministerien und die Polizei

Webseiten mehrerer Ministerien in Sachsen-Anhalt und Mecklenburg-Vorpommern sind angegriffen worden, angeblich auch von russischen Hackern. In Niedersachsen waren zudem Internetseiten der Polizei betroffen.

04.04.2023, 20.05 Uhr

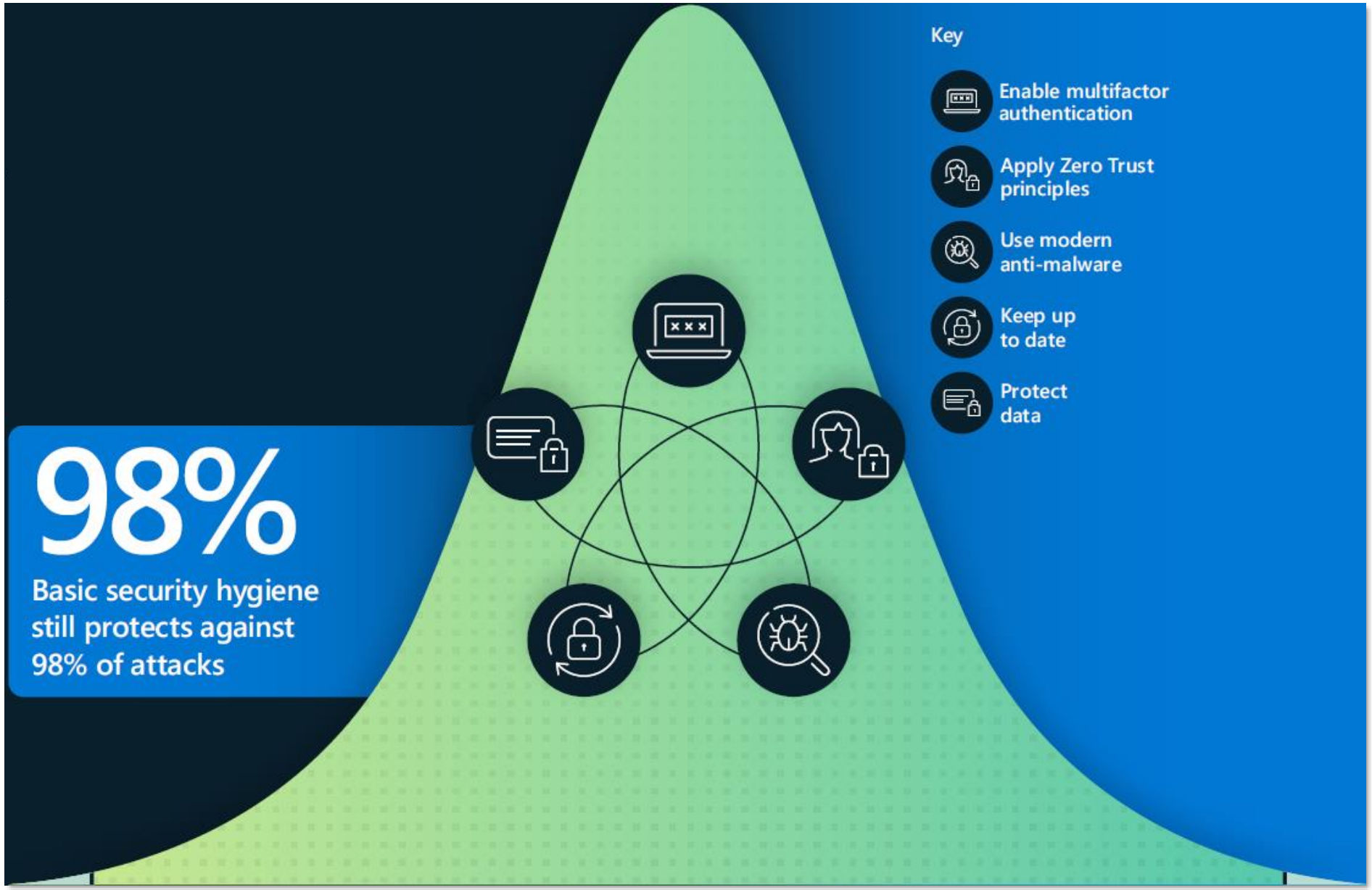
Quelle: Spiegel Online

Microsoft Digital Defense Report

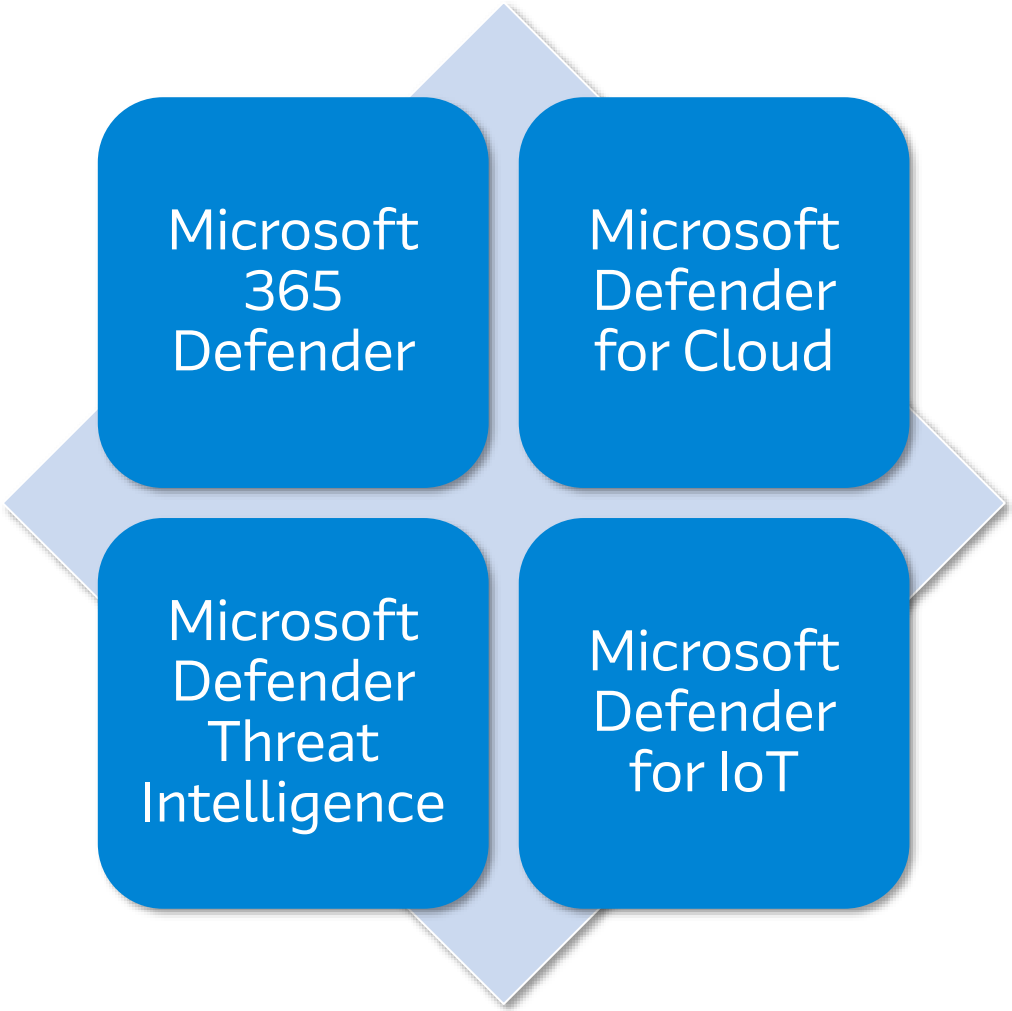


https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

Microsoft Digital Defense Report



Microsoft Defender



Microsoft 365 Defender

Microsoft

- Microsoft Defender for Endpoint
- (Microsoft Defender for Business)
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity

	Information Worker Plans												Frontline Worker Plans					
	Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 11			Microsoft 365					Office 365
	E3	E5	E5 Security[1]	E5 Compliance[1]	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security[2]	F5 Compliance[2]	F5 Sec+Comp[2]	F3
Information protection																		
Azure Information Protection Plan 1	•							•					•	•				
Azure Information Protection Plan 2		•		•					•							•	•	
Manual, default, and mandatory sensitivity labeling in Microsoft 365	•	•				•	•	•	•				•[1]	•				
Automatic sensitivity labeling in Microsoft 365 apps		•		•			•		•							•	•	
Manual labeling with the AIP app and plugin	•	•						•	•				•	•				
Automatic labeling in the AIP plugin		•		•					•							•	•	
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive		•		•			•									•	•	
Sensitivity labels based on Machine Learning/Trainable Classifiers		•		•												•	•	
Sensitivity labeling for containers in Microsoft 365	•	•				•	•							•				
Basic Message Encryption	•	•				•	•	•[2]	•[2]				•[2]	•				
Advanced Message Encryption		•		•			•		•[2]							•	•	
Customer Key		•		•			•									•	•	
Personal Data Encryption	•	•									•	•		•				
Data loss prevention (DLP)																		
DLP for emails & files	•	•				•	•									•	•	
DLP for Teams chat		•		•			•									•	•	
Endpoint DLP		•		•												•	•	
Threat protection																		
Microsoft Defender Antimalware	•	•									•	•		•				•
Microsoft Defender Firewall	•	•									•	•		•				
Microsoft Defender Exploit Guard	•	•									•	•		•				
Microsoft Defender Credential Guard	•	•									•	•		•				
BitLocker and BitLocker To Go	•	•									•	•		•				
Microsoft Defender for Endpoint Plan 1	•	•																
Microsoft Defender for Endpoint Plan 2		•	•									•			•		•	
Microsoft Defender for Identity		•	•						•						•		•	
Microsoft Defender for Office 365 Plan 2		•	•				•								•		•	
Microsoft Defender Application Guard for Edge	•	•									•	•		•				
Microsoft Defender Application Guard for Office		•	•												•		•	
Safe Documents		•	•												•		•	

[1] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).

[2] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).

[1] Microsoft 365 F1 does not include Exchange email service or Microsoft 365 apps.

[2] Does not include Exchange email service.

	Information Worker Plans												Frontline Worker Plans					
	Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 11			Microsoft 365					Office 365
	E3	E5	E5 Security[1]	E5 Compliance[1]	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security[2]	F5 Compliance[2]	F5 Sec+Comp[2]	F3
Cloud access security broker																		
Microsoft Defender for Cloud Apps Discovery	•	•						•	•				•	•				
Microsoft Defender for Cloud Apps		•	•	•					•						•	•	•	
Office 365 Cloud App Security			•	•			•		•						•	•	•	
Identity and access management																		
Azure Active Directory Premium Plan 1	•							•					•	•				
Azure Active Directory Premium Plan 2		•	•						•						•		•	
User Provisioning	•	•	•		•	•	•	•	•				•	•	•		•	•
Cloud user self-service password change	•	•	•		•	•	•	•	•				•	•	•		•	•
Cloud user self-service password reset	•	•	•					•	•				•	•	•		•	
Hybrid user self-service password change/reset with on-premises write-back	•	•	•					•	•				•	•	•		•	
Advanced Security Reports	•	•	•					•	•				•	•	•		•	
Multi Factor Authentication	•	•	•		•	•	•	•	•				•	•	•		•	•
Conditional Access	•	•	•					•	•				•	•	•		•	
Risk Based Conditional Access / Identity Protection		•	•						•						•		•	
Privileged Identity Management		•	•						•						•		•	
Access Reviews		•	•						•						•		•	
Entitlement Management		•	•						•						•		•	
Microsoft 365 Groups	•	•			•	•	•							•				•
On-premises Active Directory sync for SSO	•	•			•	•	•	•	•				•	•	•		•	•
DirectAccess supported	•	•									•	•		•				
Windows Hello for Business	•	•								•	•	•		•				
Microsoft Advanced Threat Analytics	•	•						•	•				•	•	•		•	
Endpoint and app management																		
Microsoft Intune Plan 1	•	•						•	•				•	•				
Mobile Device Management	•	•			•	•	•	•	•	•	•	•	•	•				
Mobile application management	•	•						•	•	•	•	•	•	•				
Windows Autopilot	•	•						•[1]	•[1]				•[1]	•				
Group Policy support	•	•				•	•											
Cloud Policy service for Microsoft 365	•	•			•[2]	•	•							•[2]				•[2]
Shared computer activation for Microsoft 365 apps	•	•				•	•											
Endpoint Analytics	•	•						•	•				•	•				
Cortana management	•	•									•	•		•				

[1] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).

[2] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).

[1] Does not include Windows license.

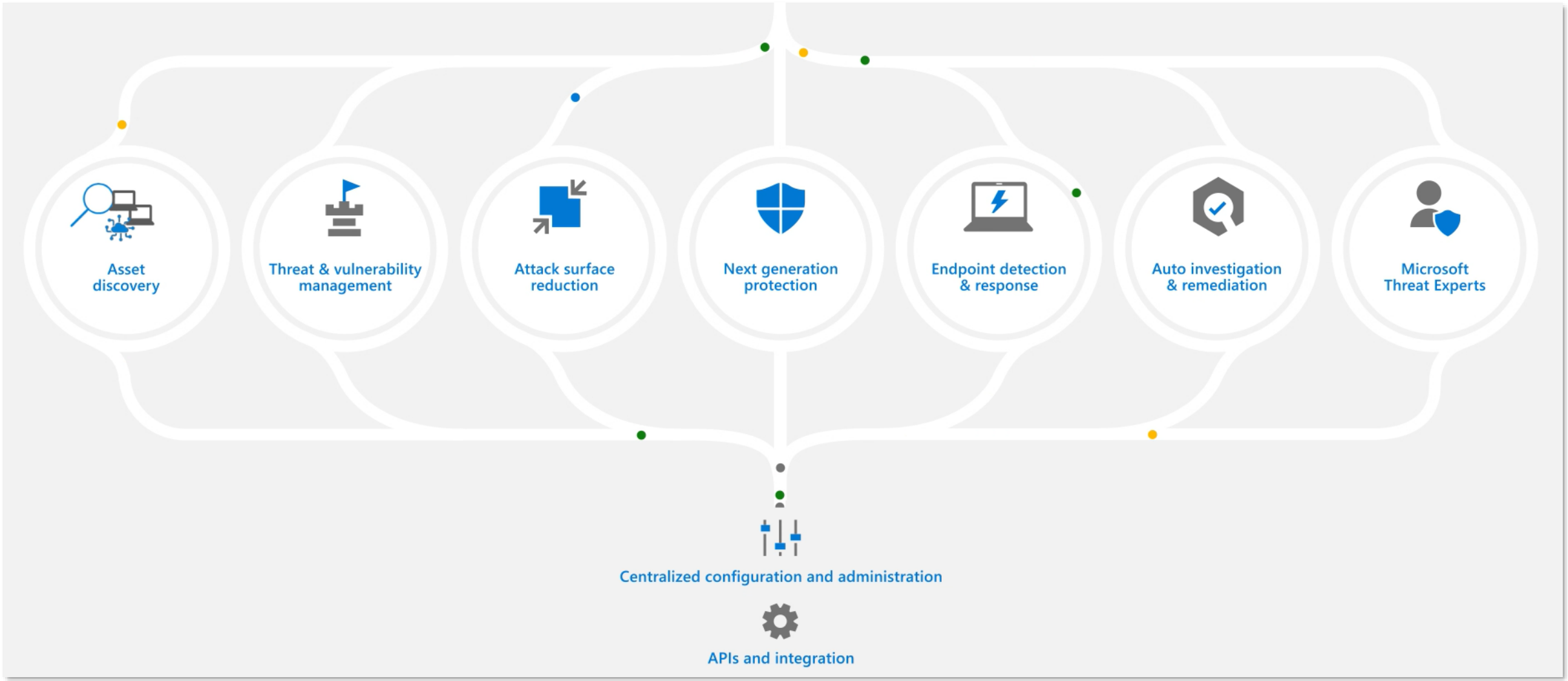
[2] Limited to policies for web apps.

Microsoft 365 Defender

Microsoft

- Microsoft Defender for Endpoint
- (Microsoft Defender for Business)
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity

Microsoft Defender for Endpoint

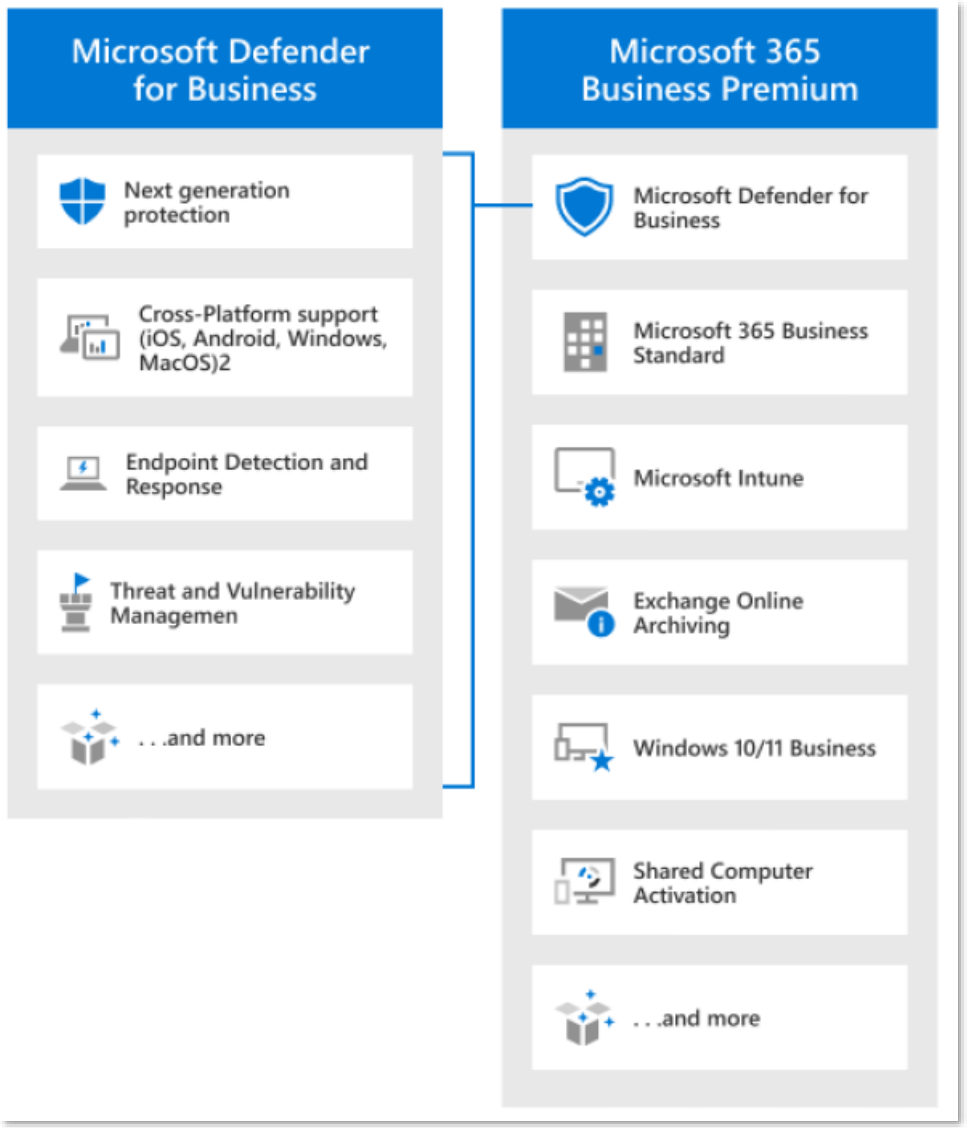


Microsoft Defender for Endpoint

Feature/Funktion	Defender für Unternehmen (eigenständig)	Defender für Endpunkt Plan 1 (für Unternehmenskunden)	Defender für Endpunkt Plan 2 (für Unternehmenskunden)
Zentralisierte Verwaltung *(siehe Hinweis 1 unten)*	✓	✓	✓
Vereinfachte Clientkonfiguration	✓		
Microsoft Defender Sicherheitsrisikomanagement	✓		✓
Funktionen zur Verringerung der Angriffsfläche *(siehe Hinweis 2 unten)*	✓	✓	✓
Schutz der nächsten Generation	✓	✓	✓
Erkennung und Reaktion am Endpunkt *(siehe Hinweis 3 unten)*	✓		✓
Automatische Untersuchung und Reaktion *(siehe Hinweis 4 unten)*	✓		✓
Bedrohungssuche und sechs Monate Datenaufbewahrung			✓
Bedrohungsanalyse *(siehe Hinweis 5 unten)*	✓		✓
Plattformübergreifender Support Windows, Mac, iOS und Android OS *(für Windows Server und Linux siehe Hinweis 6 unten)*	✓	✓	✓
Microsoft-Bedrohungsexperten			✓
Partner-APIs	✓	✓	✓
Microsoft 365 Lighthouse Integration (Zum Anzeigen von Sicherheitsvorfällen über Kundenmandanten hinweg)	✓	✓	✓

https://learn.microsoft.com/de-de/microsoft-365/security/defender-business/compare-mdb-m365-plans?view=o365-worldwide

Microsoft Defender for Business



https://learn.microsoft.com/de-de/microsoft-365/security/defender-business/compare-mdb-m365-plans?view=o365-worldwide

Gartner

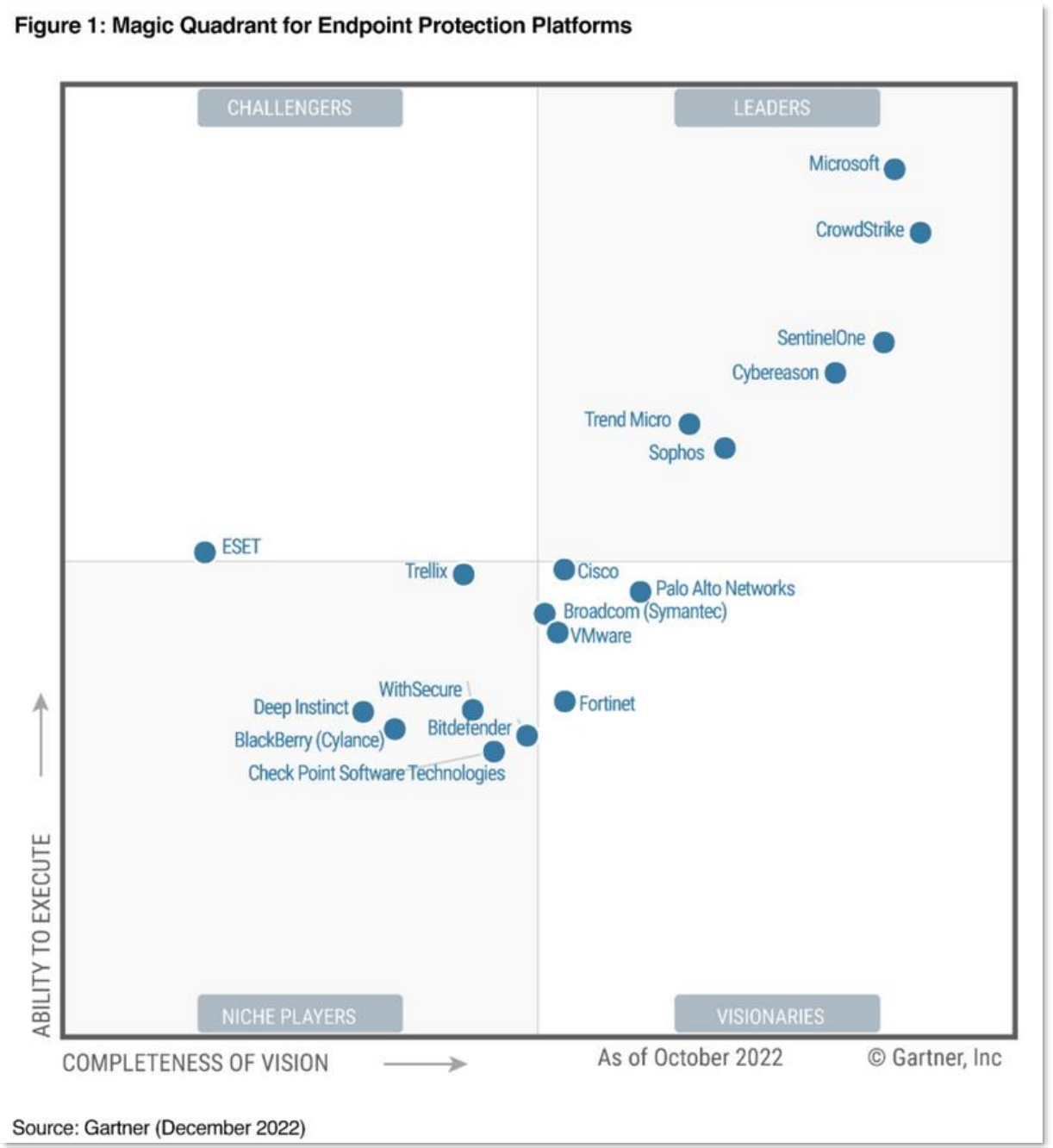


Figure 1: Magic Quadrant for Endpoint Protection Platforms
CHALLENGERS
LEADERS
Microsoft
CrowdStrike
SentinelOne
Cybereason
Trend Micro
Sophos
ESET
Trellix
Cisco
Palo Alto Networks
Broadcom (Symantec)
VMware
WithSecure
Deep Instinct
Bitdefender
BlackBerry (Cylance)
Fortinet
Check Point Software Technologies
NICHE PLAYERS
VISIONARIES
ABILITY TO EXECUTE
COMPLETENESS OF VISION
As of October 2022
© Gartner, Inc
Source: Gartner (December 2022)

Microsoft 365 Defender

Microsoft

Microsoft Defender for Endpoint

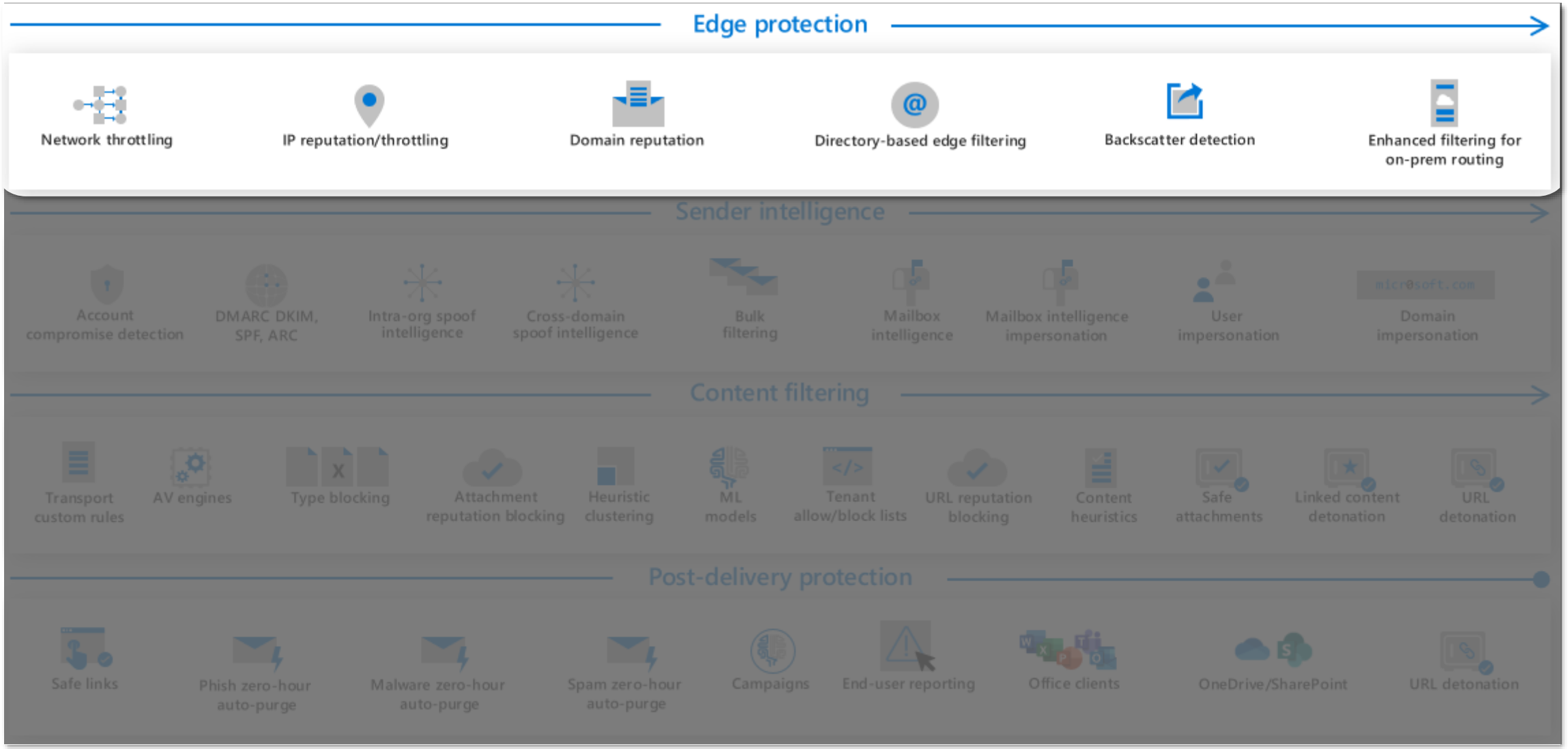
(Microsoft Defender for Business)

Microsoft Defender for Office 365

Microsoft Defender for Cloud Apps

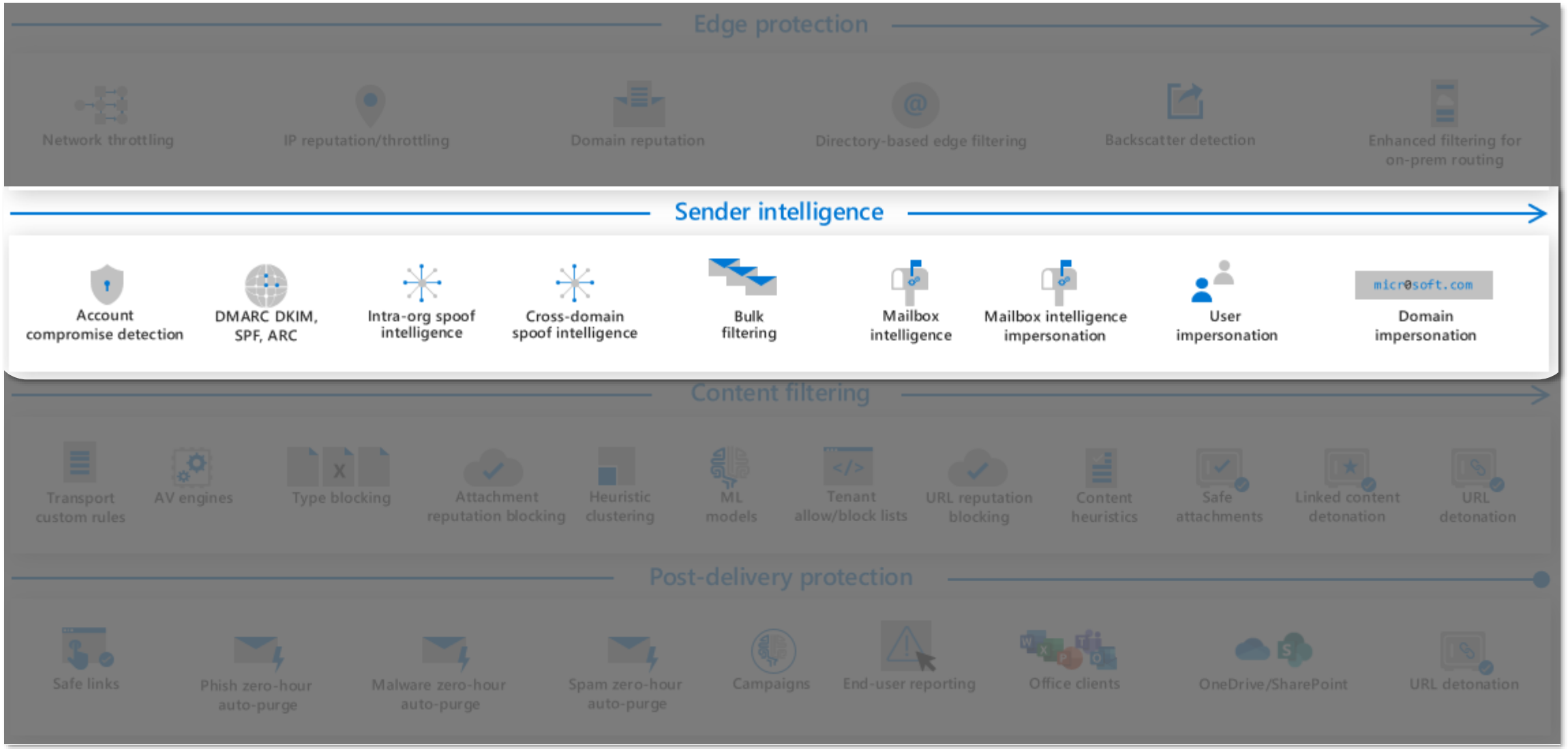
Microsoft Defender for Identity

Microsoft Defender for Office 365



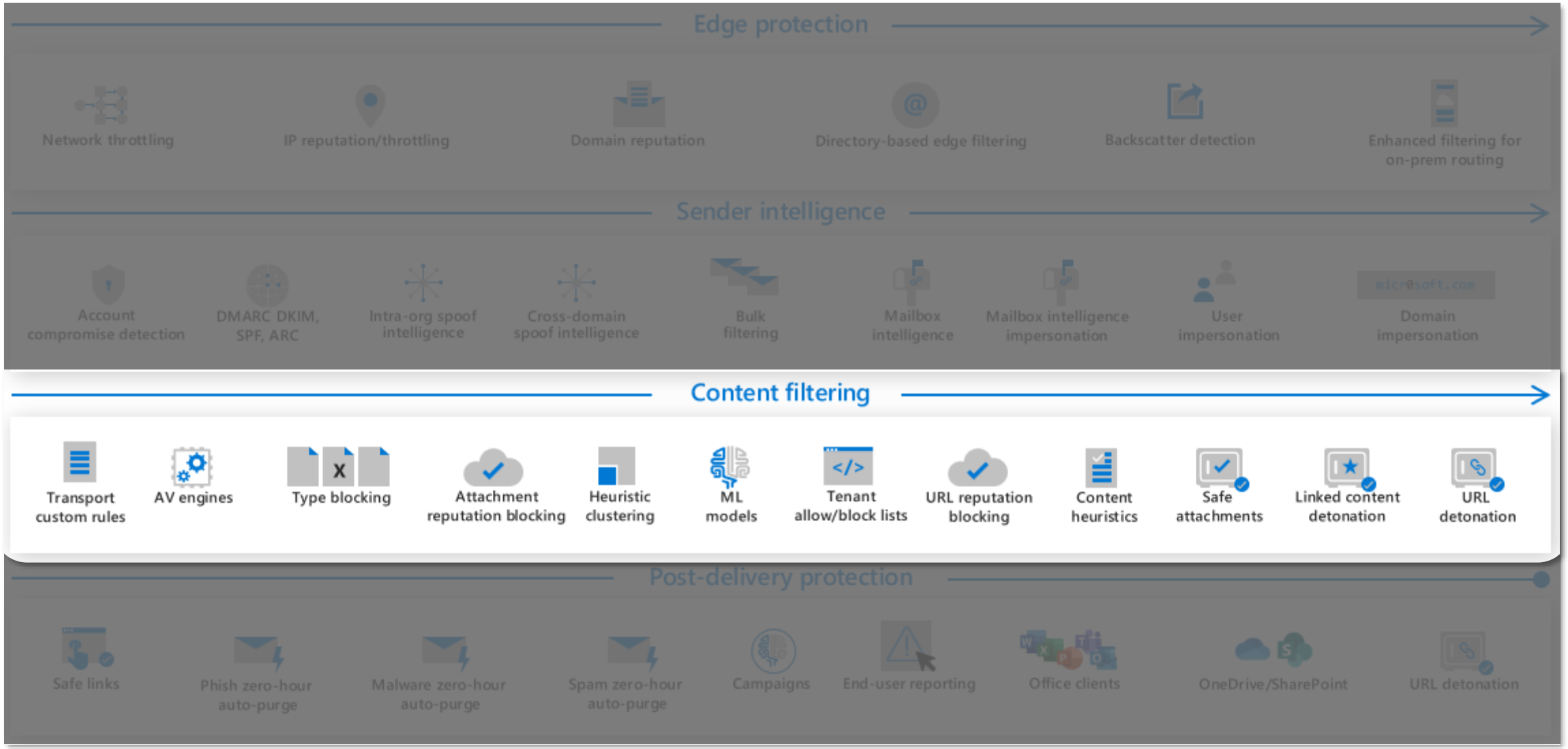
https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/protection-stack-microsoft-defender-for-office365?view=o365-worldwide

Microsoft Defender for Office 365



https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/protection-stack-microsoft-defender-for-office365?view=o365-worldwide

Microsoft Defender for Office 365

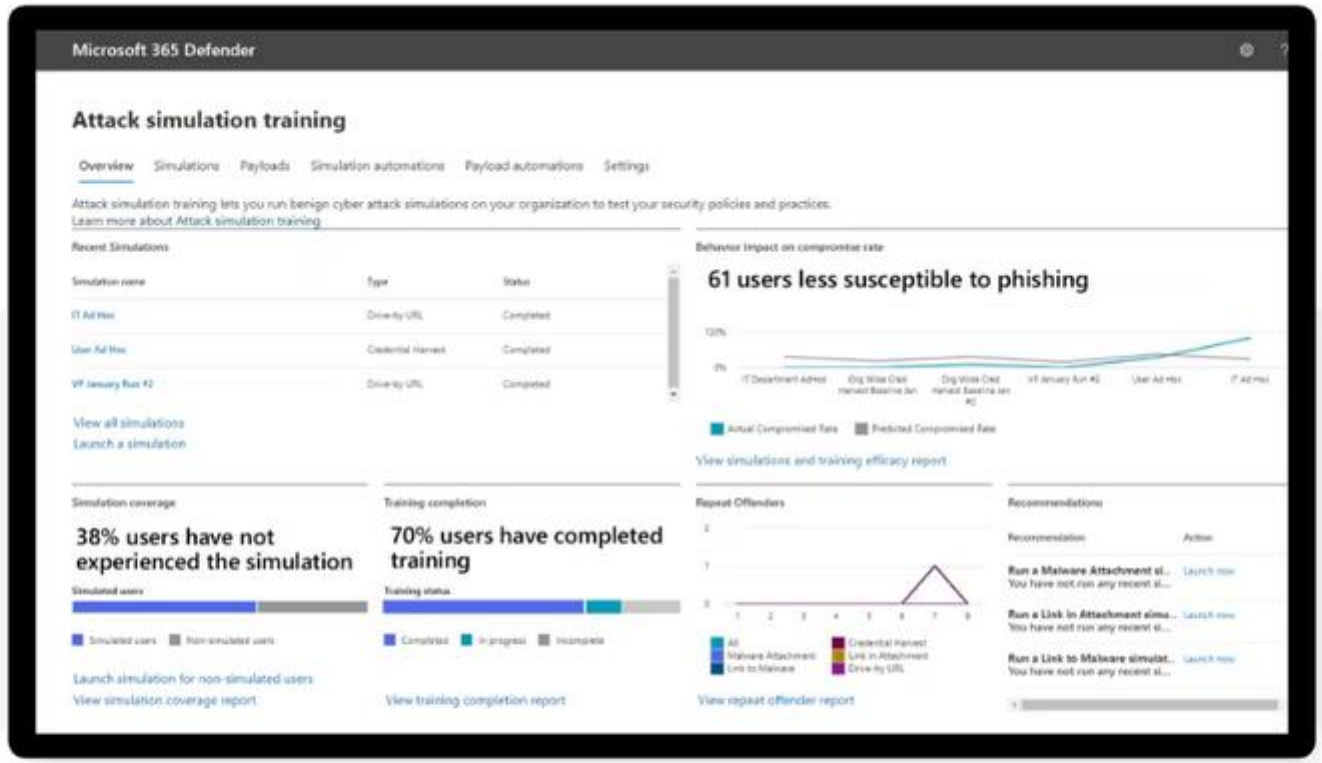


https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/protection-stack-microsoft-defender-for-office365?view=o365-worldwide

Microsoft Defender for Office 365

https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/protection-stack-microsoft-defender-for-office365?view=o365-worldwide

Microsoft Defender for Office 365



Sensibilisierung und Schulung

Sensibilisieren Sie die Endnutzer durch praxisnahe Simulationen und Schulungen sowie durch integrierte Funktionen direkt in den Clientanwendungen.

https://www.microsoft.com/de-de/security/business/threat-protection/attack-simulation-training

Microsoft 365 Defender

Microsoft Defender for Endpoint

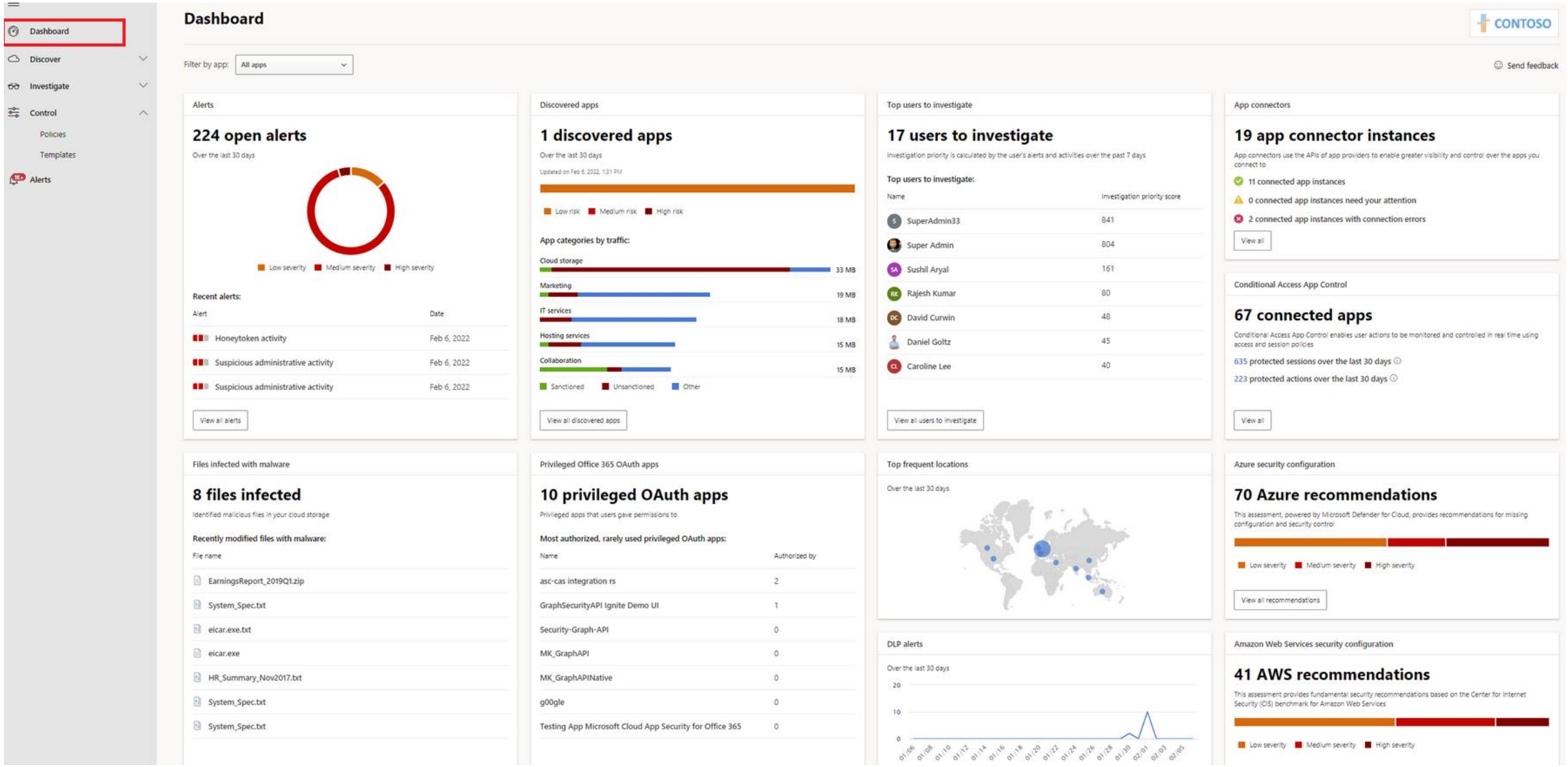
(Microsoft Defender for Business)

Microsoft Defender for Office 365

Microsoft Defender for Cloud Apps

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps



Microsoft 365 Defender

Microsoft

Microsoft Defender for Endpoint

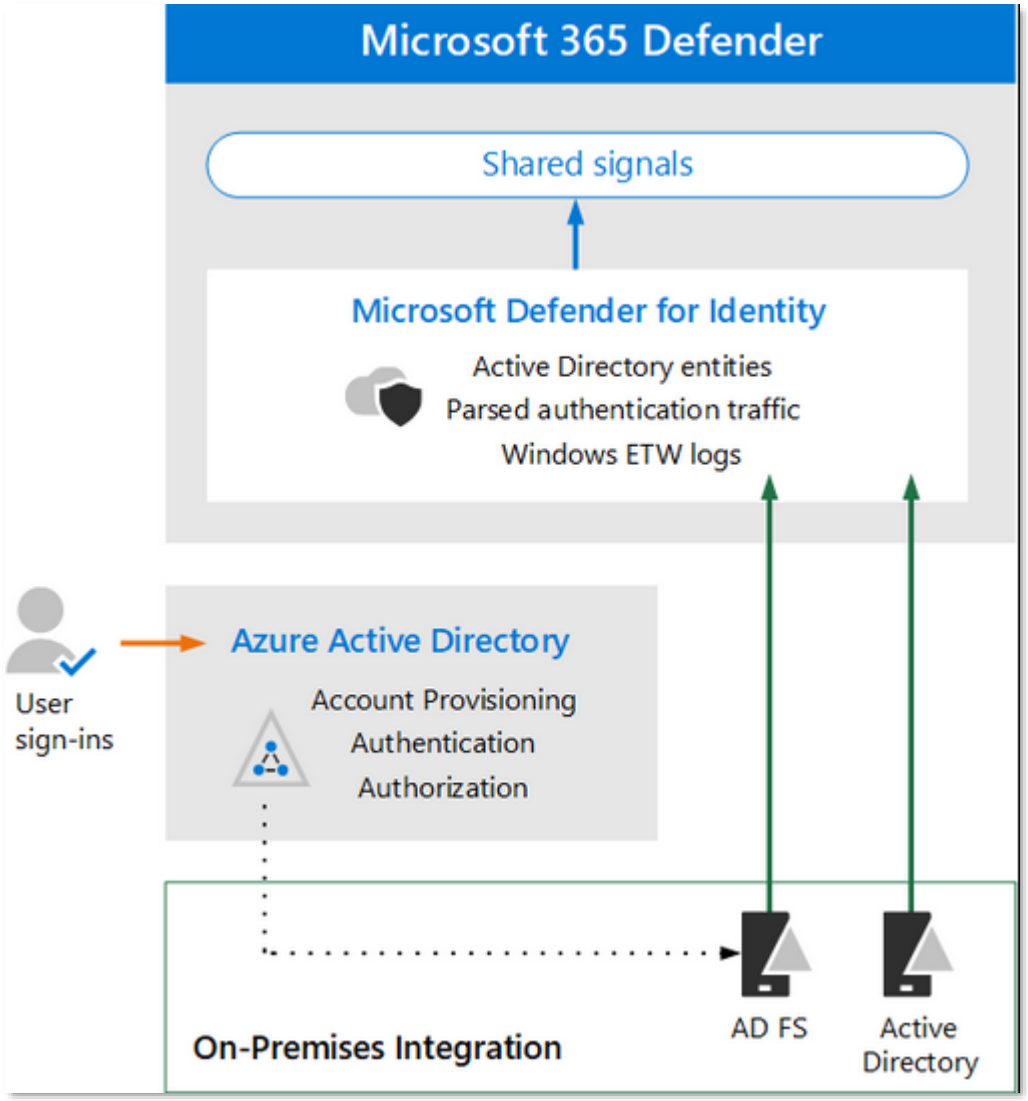
(Microsoft Defender for Business)

Microsoft Defender for Office 365

Microsoft Defender for Cloud Apps

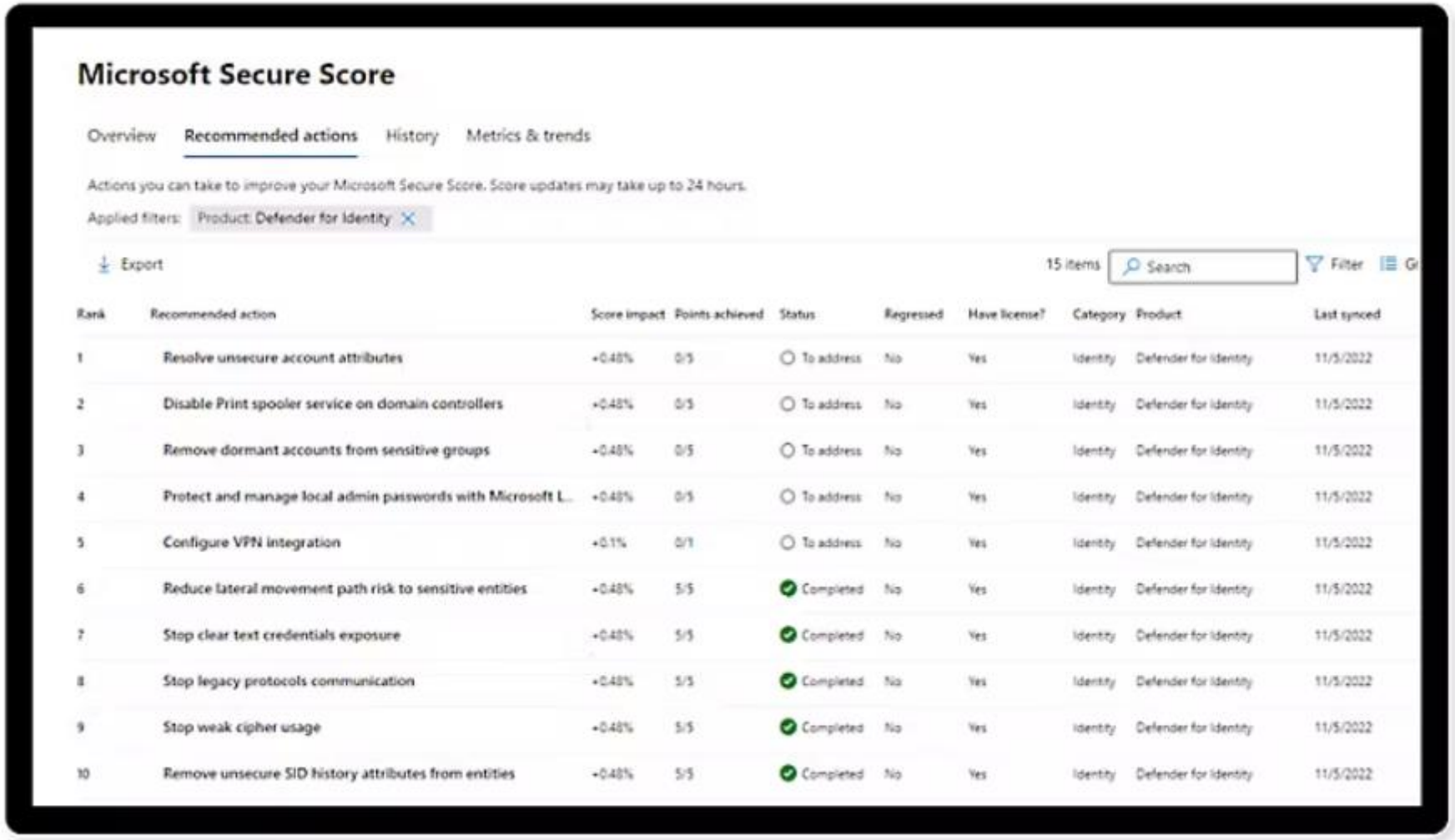
Microsoft Defender for Identity

Microsoft Defender for Identity



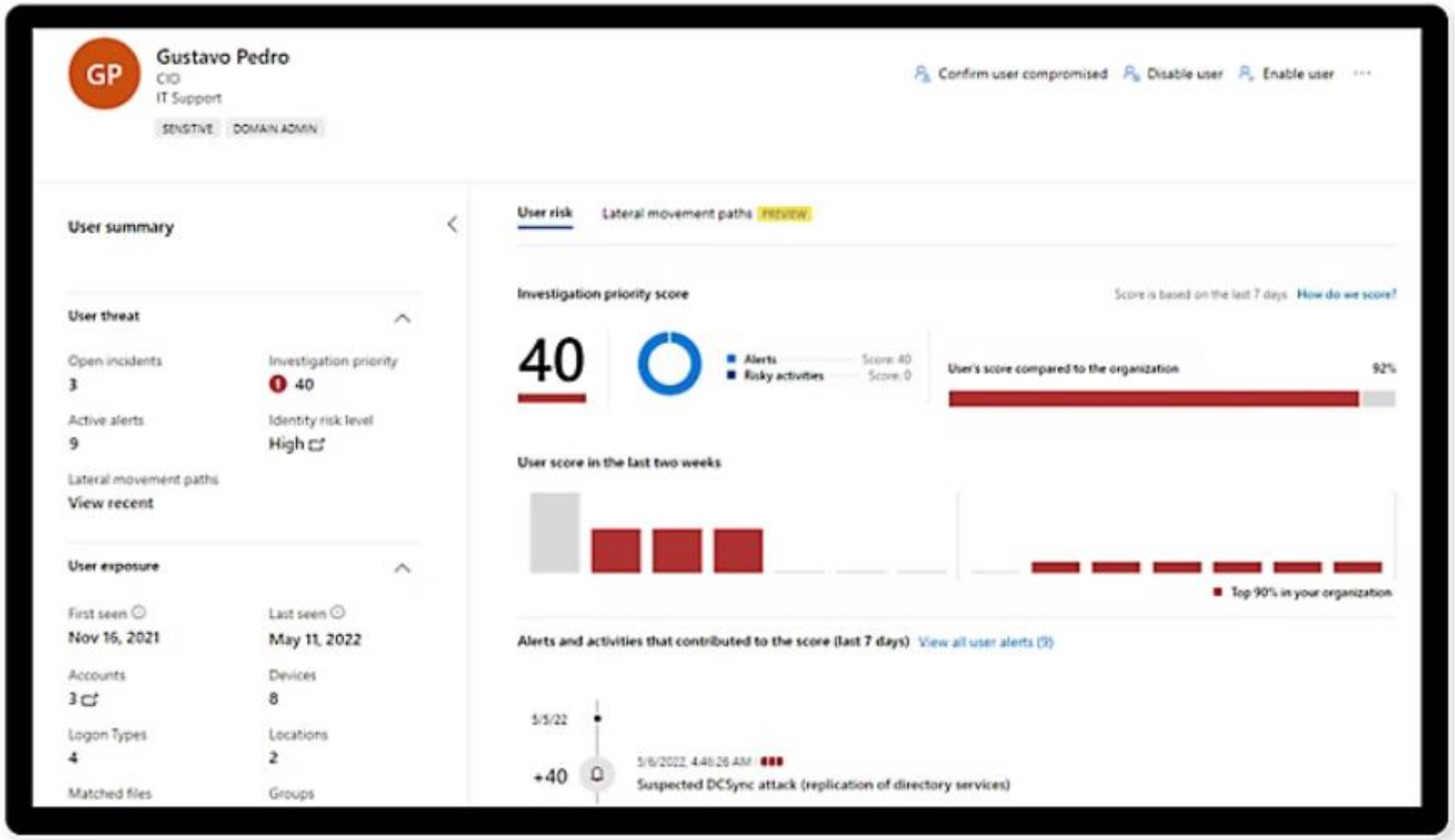
https://learn.microsoft.com/de-de/microsoft-365/security/defender/eval-defender-identity-architecture?view=o365-worldwide

Microsoft Defender for Identity



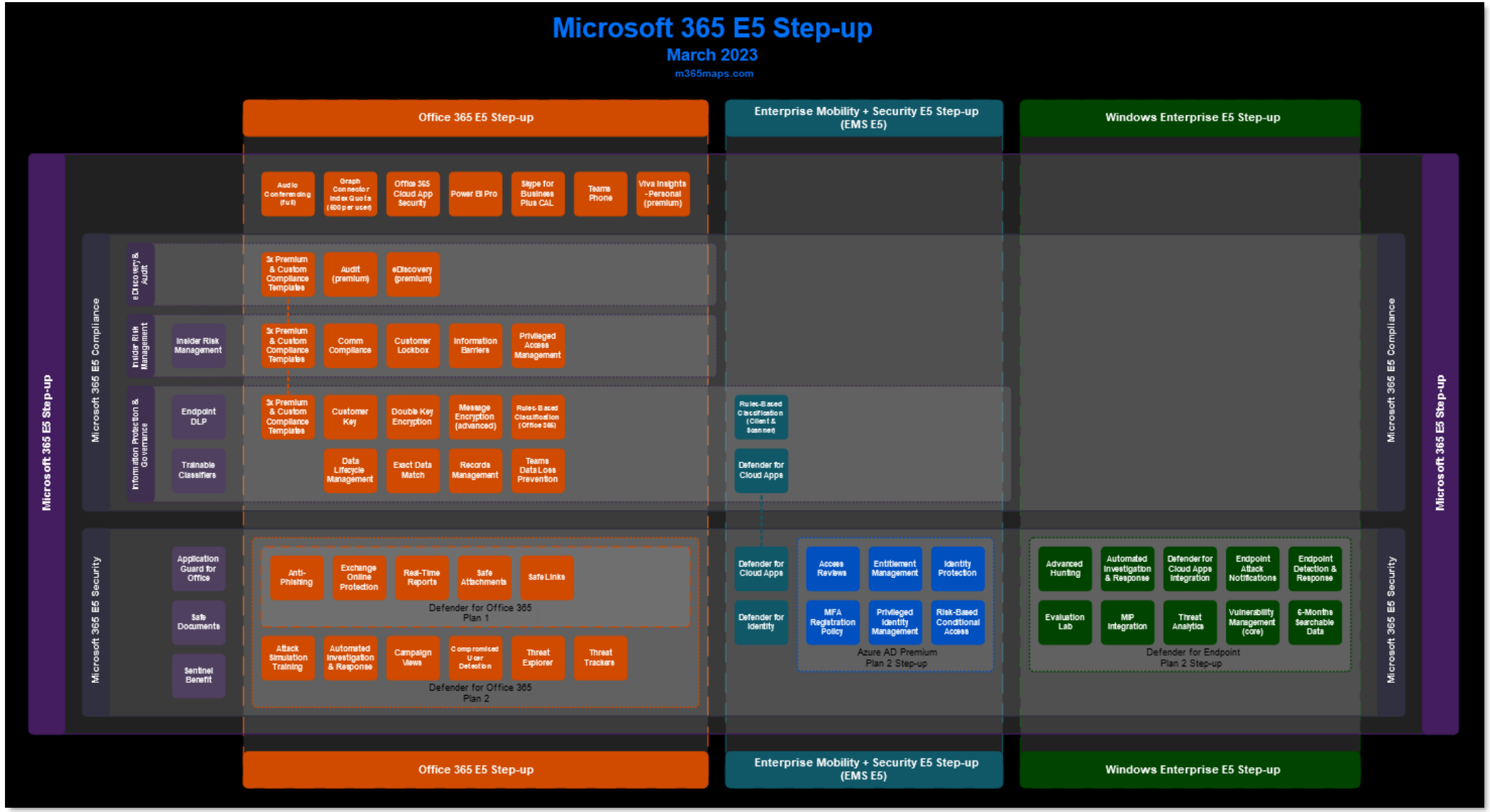
https://www.microsoft.com/de-de/security/business/siem-and-xdr/microsoft-defender-for-identity

Microsoft Defender for Identity



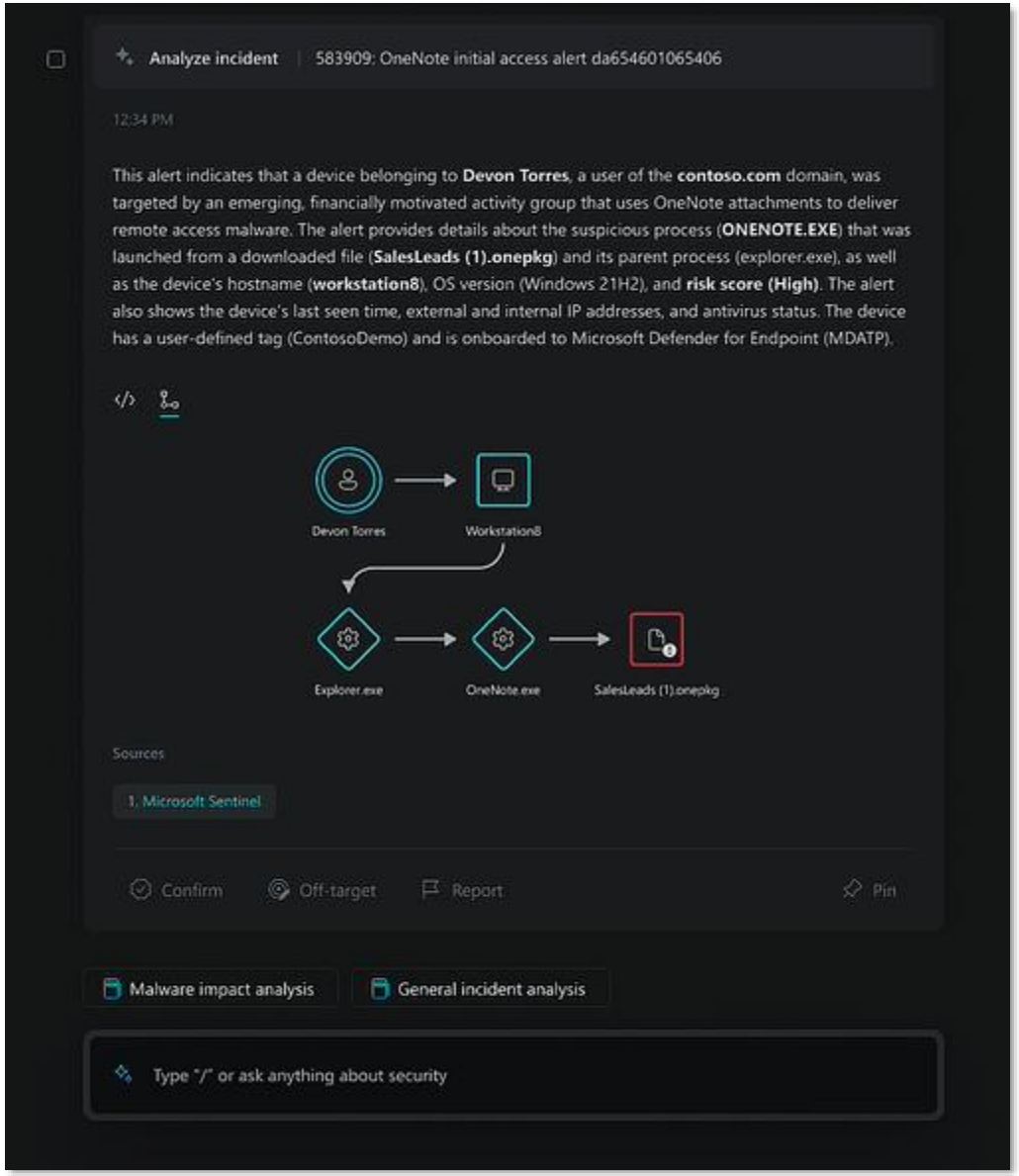
https://www.microsoft.com/de-de/security/business/siem-and-xdr/microsoft-defender-for-identity

Übersicht Lizenzierung



https://m365maps.com/

Microsoft Security Co-Pilot



https://www.microsoft.com/de-de/security/business/ai-machine-learning/microsoft-security-copilot

Zusammenarbeit mit Arrow im Bereich Microsoft

Team Microsoft

Manager Microsoft

Microsoft
Modern Work

Sebastian Weiß
+49 (0) 89 / 93099-446
+49 (0) 175 / 5755 385
sebastian.weiss@arrow.com

Business Development Manager

Microsoft

Thomas Schottenheim
+49 (0) 89 / 93099-332
+49 (0)151 / 1803 1783
thomas.schottenheim@arrow.com

Microsoft
Microsoft Azure

tba
+49 (0) 89 / 93099-xxx
@arrow.com

Program Manager

Microsoft

Nadine Mucke
+49 (0) 89 / 93099-275
+49 (0) 175 / 5755 275
nadine.mucke@arrow.com

Focus Account Manager

Microsoft

Waldemar Gert
+49 (0) 89 / 93099-181
+49 (0) 171 / 2695 672
waldemar.gert@arrow.com

Azure Solution Architect

Microsoft
Microsoft Azure

Tim Reuter
+49 (0) 89 / 93099-138
tim.reuter@arrow.com

Focus Sales

Microsoft
BitTitan

Fatma Yildirim
PLZ 8
+49 (0) 89 / 93099-116
fatma.yildirim@arrow.com

Microsoft
BitTitan

Edgar Becker
PLZ 4-6
+49 (0) 89 / 93099-375
edgar.becker@arrow.com

Microsoft
BitTitan

Sandra Deppe
PLZ 7, 9
+49 (0) 89 / 93099-264
sandra.deppe@arrow.com

Microsoft
BitTitan

Elhem Ben Hay
PLZ 0-3
+49 (0) 89 / 93099-382
elhem.benhay@arrow.com

Thank You

Thomas Schottenheim
Business Development Manager Microsoft Security
+49 (0) 89 / 93099-332
+49 (0)151 / 1803 1783
thomas.schottenheim@arrow.com