kontron

Explore the Kontron Group

We are a fast-moving multinational technology leader.

Közelmúlt biztonsági kihívásai és a lehetséges válaszok

Microsoft security

Tatár Ákos
Microsoft szegmens
Microsoft pre-sales konzulens

Microsoft Üzletág

Minősítések és referenciák

kontron

- Több mint 20 Microsoft Certified mérnök - és további 20 fejlesztő
- Solution Partner minősítések - Infrastructure, Security and Modern Work , Data/ AI, Digital and App Innovation
- Advanced Specialization minősítések
  - Windows Server and SQL Server Migration to Microsoft Azure
  - Adoption and Change Management
  - Teamwork Deployment
  - Identity and Access Management
  - Information Protection and Governance
  - Threat Protection
- 10 év tapasztalat Microsoft alapú felhő termékek implementálásában
  - 2013: Európában az első Azure Managed Service Provider
  - “Microsoft Partner of the Year” díj 2017, 2020 és 2022-ben
- Cloud Solution Provider és Microsoft FastTrack Partner

GRAPHISOFT A NEMETSCHEK COMPANY
HBO
Lufthansa Systems
AMC
Brendon
MAGYAR KÖZÚT
FKF
Országos Bírósági Hivatal
Magyar Posta
affidea
RICHTER GEDEON
KUKA
otpbank
NNG
SEMILAB
Fundamenta Lakáskassza
tv2.hu
ebiz by OTP Business
Euronet WORLDWIDE
SZERENCSEJÁTÉK ZRT.

Kihívások és trendek az IT biztonságban

A biztonság sosem volt ennyire fontos

A kibertámadások **gyakorisága és szofisztikáltsága egyre növekszik**

Ez a nyomás csak fokozódik a **hibrid** és **multi-cloud környezetekben**

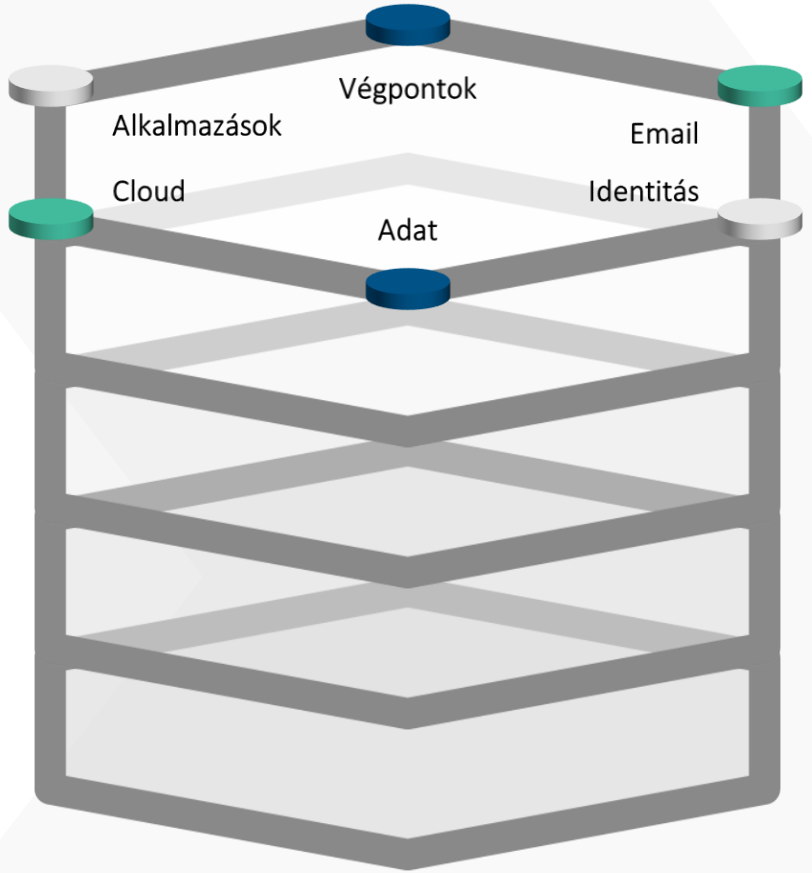
Egyre összetettebb a szabályozási környezet

- Vizibilitás növelése
- Folyamatos kontroll és rálátás
- Kockázatok feltárása és kezelése - **proaktivitás**

- Együttműködés
- Összefüggések feltárása
- Automatizált válaszlépések

Trendek

A biztonság átfogó megközelítése, vendor konszolidáció



Biztonság

Megfelelés

Identitás

Végpont menedzsment

Adatvédelem

Multi-cloud & multi-platform, hibrid

Mit nyújt a Microsoft?

Zero Trust megközelítés

kontron

Pontos ellenőrzés

Minden rendelkezésre álló adat ellenőrzése

- Felhasználói identitás és elhelyezkedés
- Eszköz egészségi állapot
- Hozzáférés típusa
- Adat típus
- Anomáliák

Minimális jogosultság elve

Az adat és a produktivitás védelmének az elősegítése a megfelelő jogosultsággal

- Just-in-time (JIT)
- Just-enough-access (JEA)
- Veszély alapú adaptív házirendek
- Hálózaton kívül közlekedő adat védelme

Felkészülni a betörésre

Minimalizálni az elérhető erőforrásokat, és megakadályozni a hálózati mozgást

- Hálózati szeparáció, alkalmazás, felhasználó és eszköz tudatosság
- Végpontok közötti titkosítás
- Elérhető adatok elemzése, sérülékenyég észlelése

Identitások – Végpontok – Adat – Alkalmazások – Infrastruktúra - Hálózat

Microsoft célmegoldások

kontron

Microsoft 365 Defender termékcsalád

M365 Defender for Identity

Biztosítja és kezeli a hybrid identitások védelmét, és egyszerűsíti az alkalmazotti, valamint a partner hozzáférést.

M365 Defender for Endpoint

Végponti veszélyforrás-észlelés, incidensek utáni védekezés, automatizált kivizsgálás és azokra történő reagálás a munkavállalói és felügyelt végpontok esetén.

M365 Defender for Cloud Apps

Láthatóságot biztosít, ellenőrzés alatt tartja az adatokat, észlelheti a veszélyforrásokat a felhőszolgáltatásokban és felhőalkalmazásokban.

M365 Defender for O365

Védelmet nyújt a teljes Office 365-nek a komplex veszélyforrások, többek között az adathalászat és az üzleti levelezés feltörése ellen.

M365 Defender for Cloud

Infrastruktúra oldali komponensek védelmét biztosítja, kiterjed kiszolgálókra, konténerekre, Azure szolgáltatásokra, IoT eszközökre, és még több egyéb elemre.

Végfelhasználók védelme

Infrastruktúra védelme

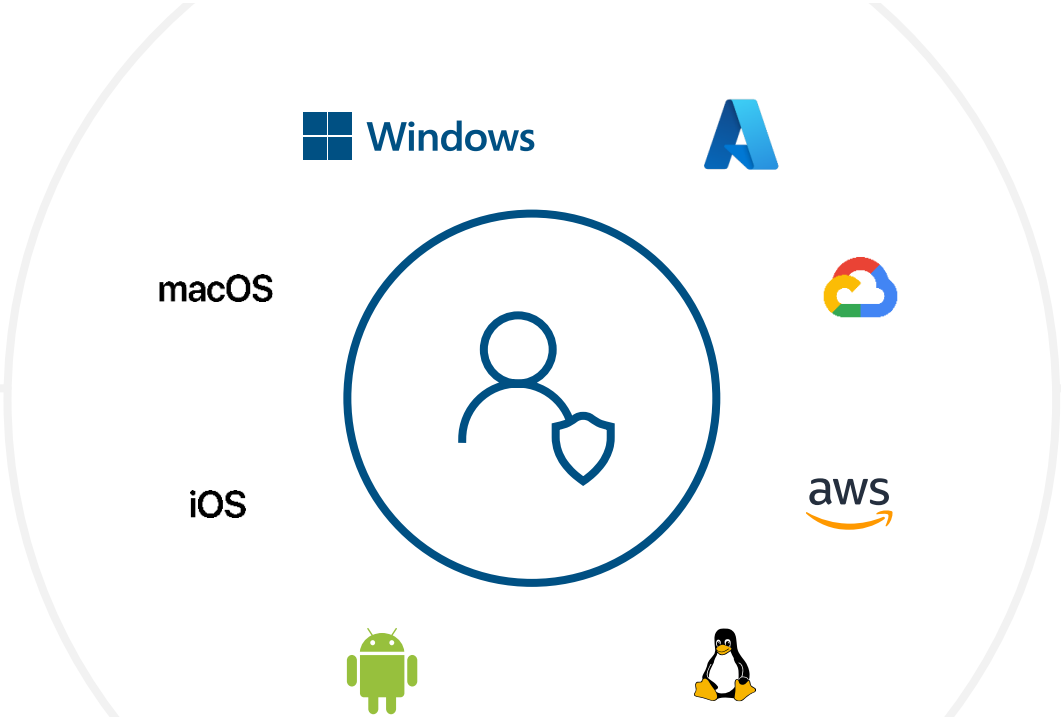
Microsoft security

kontron

SIEM

Microsoft Sentinel

Vizibilitás az egész szervezeten belül



Meglévő biztonsági portfólió

Microsoft ökoszisztéma

Microsoft 365 Defender

Végfelhasználók védelme

Microsoft Defender for Cloud

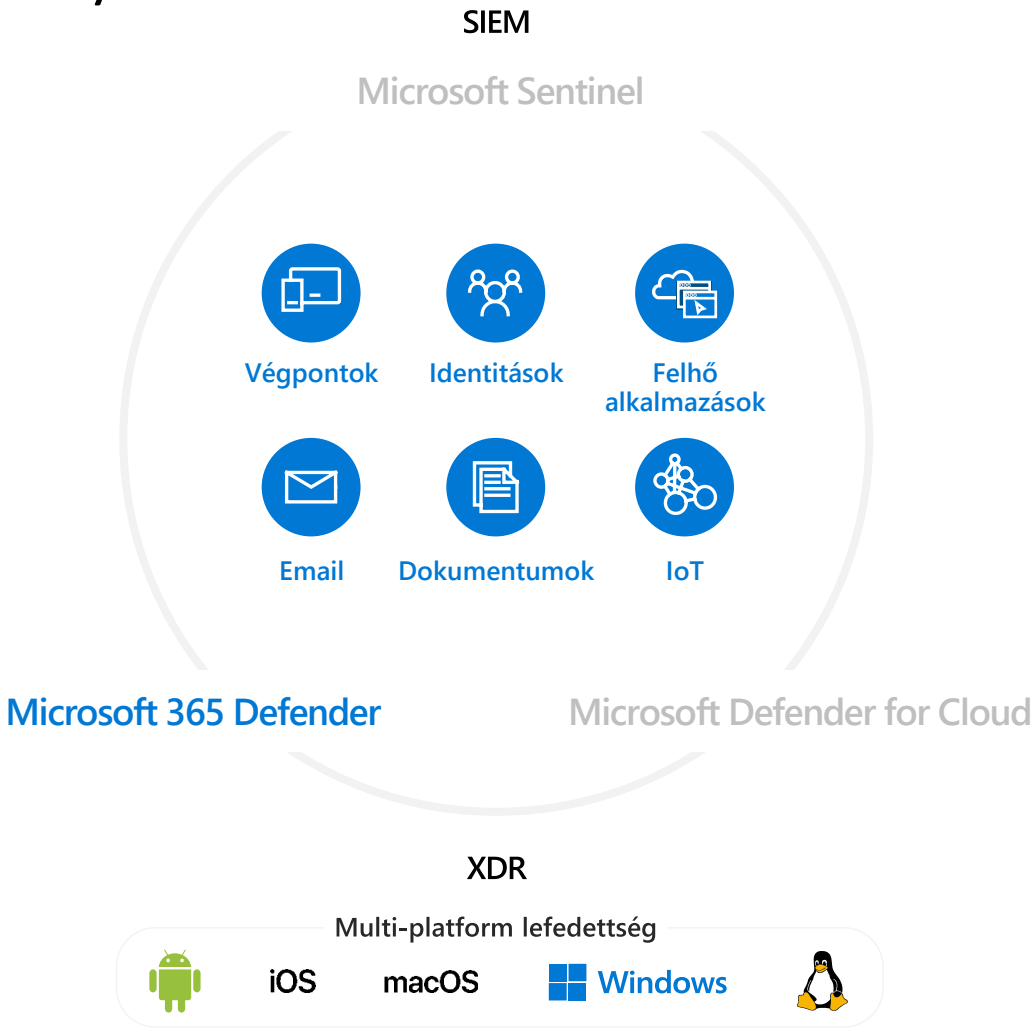
Infratruktúra védelme

XDR

Végfelhasználók védelme XDR segítségével

A támadások megállítása és a válaszlépések hatékony koordinálása

- Fejlett és szofisztikált támadások megelőzése minőségi védelemmel.
- Windows, MacOS, Linux, Android és iOS eszközök védelme.
- Email alapú támadások elleni védelem.
- Tartományokon és szervezeteken átívelő integrált biztonság.
- Incidens vizsgálat, sérülékenységek keresése és kezelése a végfelhasználói környezetben egy központi felületről.



Multi-cloud védelme XDR segítségével

Iparág vezető XDR képesség a fenyegetések ellen

- On-prem, Azure, AWS és Google Cloud erőforrások védelme.
- Rossz indulatú szoftverek és támadások elleni védelem Windows vagy Linux kiszolgálóknak, függetlenül attól, hogy a felhőben vagy on-prem helyezkednek el.
- Sérülékenységek vizsgálat és ezáltal a támadások megelőzése.
- Adatszolgáltatások védelme.

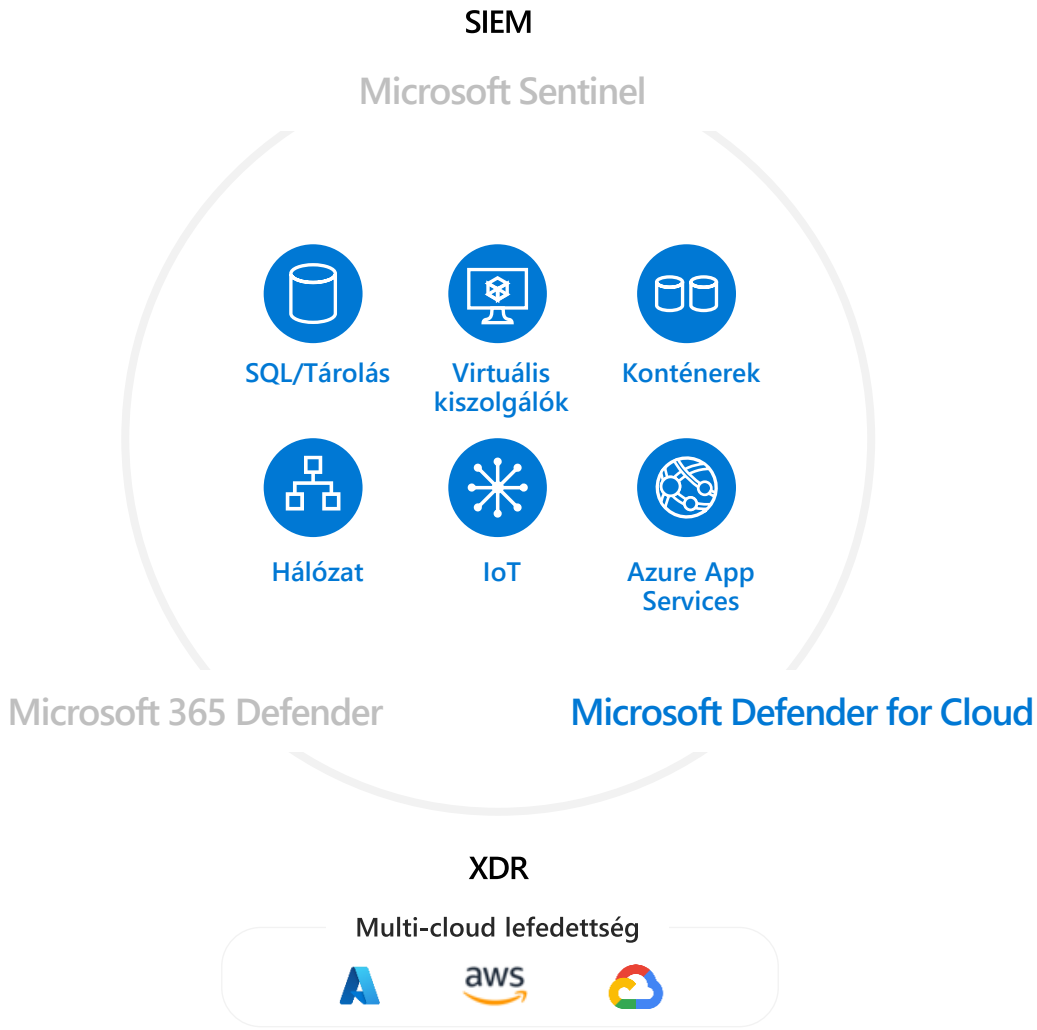


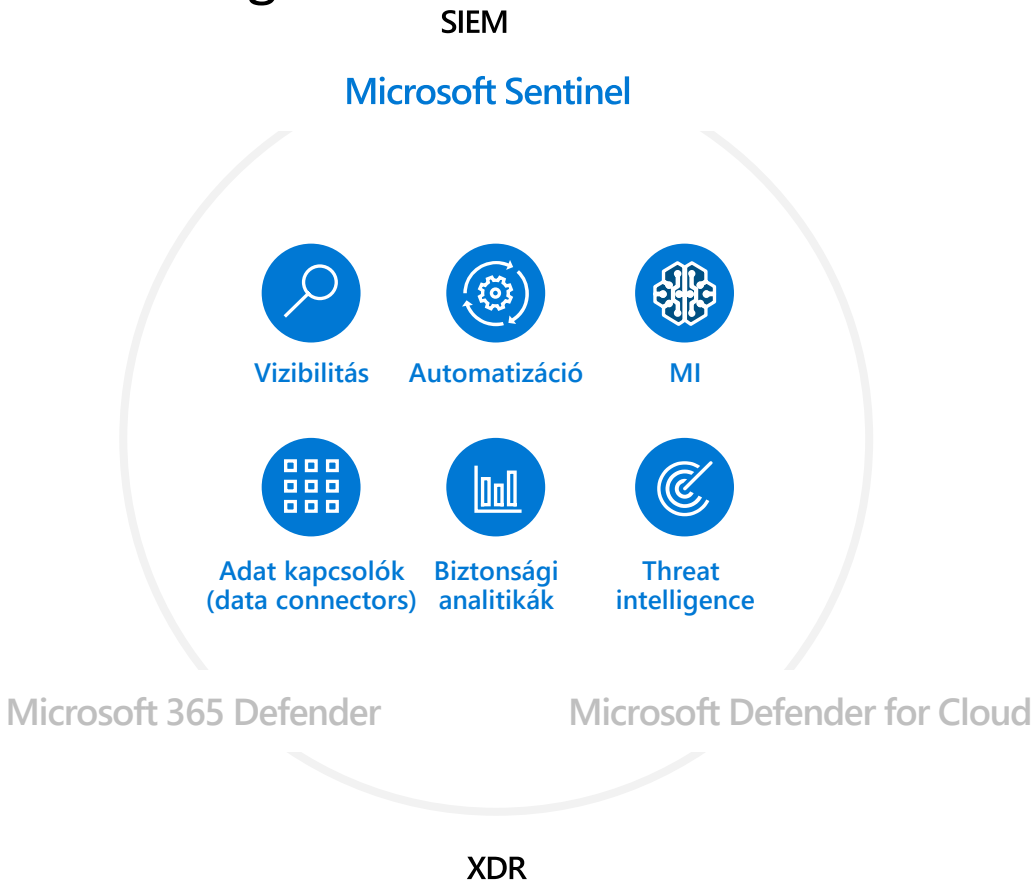
Figure 1: Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (December 2022)

Microsoft Sentinel

Optimalizált biztonság az Azure natív, MI vezérelt SIEM megoldásával

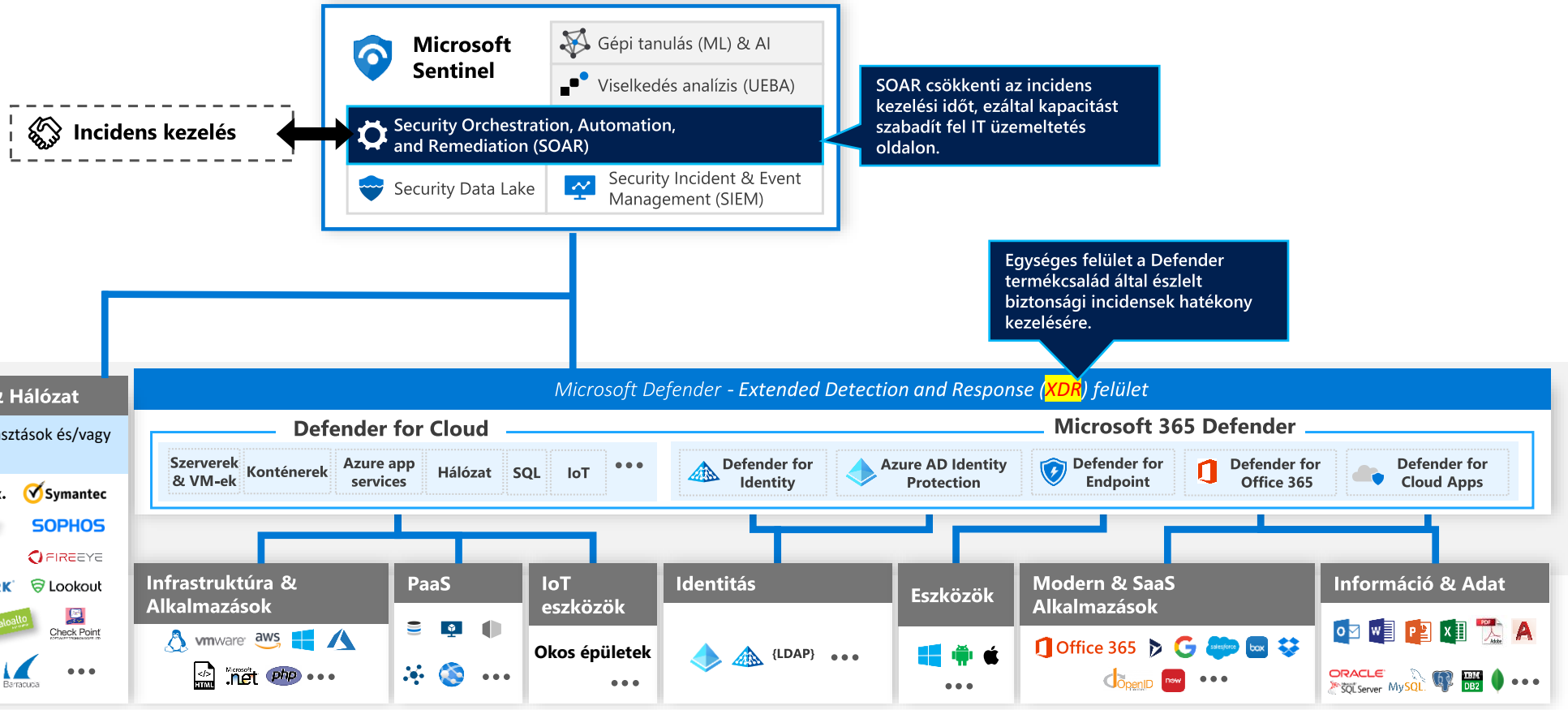
- Az adatok felhő szintű gyűjtése és analizálása, meglévő eszközök integrálása a “data connectors” segítségével.
- Teljes analízis a Threat Intelligence, viselkedés elemzés, gépi tanulás és a Microsoft több évtizedes tapasztalatai alapján.
- Incidensek esetén a válaszidő csökkentése a beépített eszközök, MI automatizáció, és SOAR funkciók segítségével.



Microsoft Kiberbiztonság Referencia Architektúra

kontron

Teljes infrastruktúra nézet
Korrelál és egységes incidens nézet (felhő és on-prem) a teljes infrastrukturára



Defender XDR
Eszköz specifikus egységes felület incidens és sérülékenység kezelésre

Nyers Adat
Security & Activity napló állományok

Összegzés

kontron

Vizibilitás növelése

- Megnő és mérhető lesz a biztonsági szint
- Kevesebb vakfolt és biztonsági rés a teljes rendszerben

+

Riasztások/incidensek kezelése

- Hatékonyabb, egyszerűbb lesz, kevesebb riasztási “zaj”
- Triázs lehetősége
- Összefüggések meghatározása (AI)
- Automatizált válaszlépések

=

Security/üzemeltető csapat

- Tehermentesítés és ezáltal hatékony működés
- Több idő jut fontosabb feladatokra
- SecOps módszertanok használata

Microsoft security

“Takeaway”

kontron

Védeni
mindent

Egyszerűsíteni
a komplexet

Látni
amit más nem

Foglalkozni
csak a fontossal

Köszönöm a figyelmet

Tatár Ákos
Microsoft pre-sales konzulens
akos.tatar@kontron.hu

Kontron Hungary Kft.
2040 Budaörs,
Puskás Tivadar út 14.
info@snt.hu
1 371 8000
www.kontron.hu