Adatvédelmi technológiák áttekintése

Hargitai Zsolt
üzletfejlesztési igazgató
zsolt.hargitai@microfocus.com

Az IT komplexitása

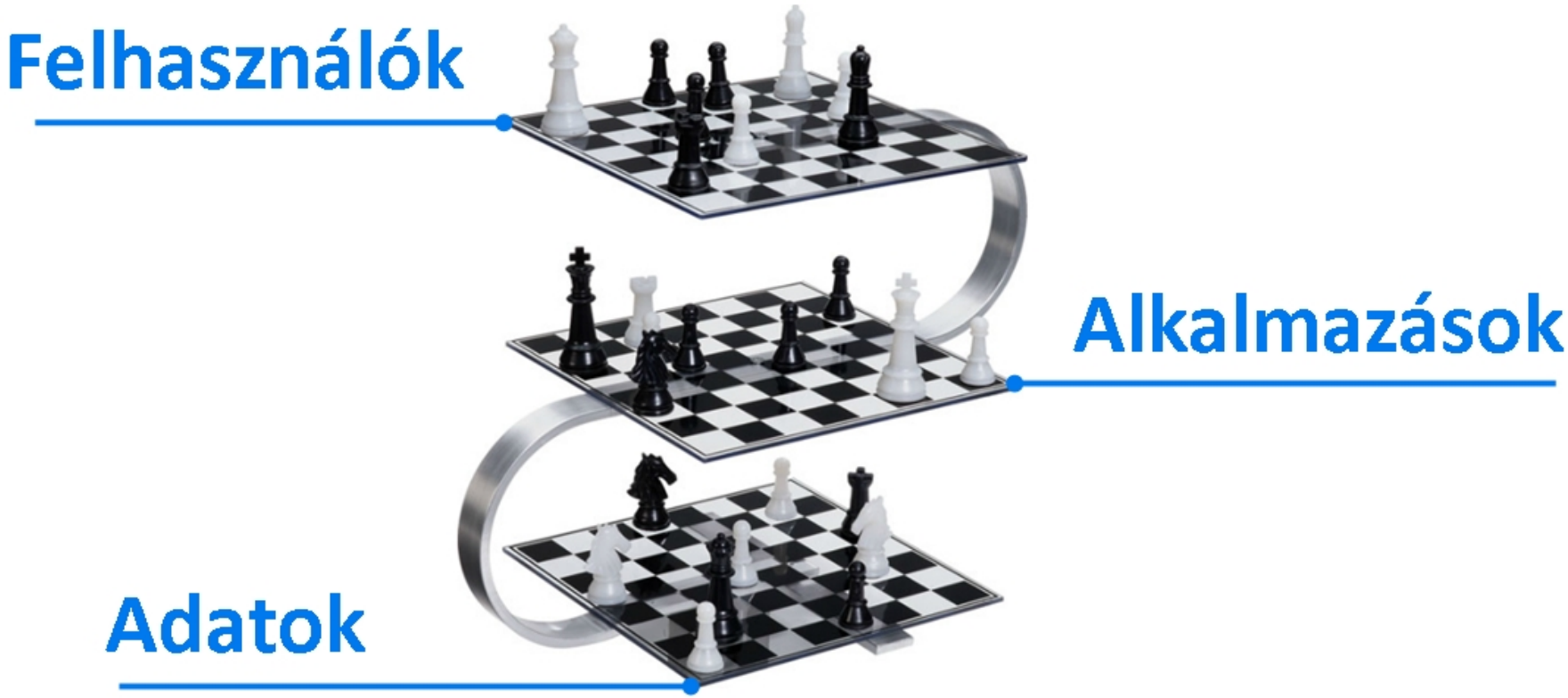
Fenyegetettség (külső és belső)

Információs túlterheltség

Szabályozás/ Törvényi megfelelés

Infrastruktúra bonyolultsága

Az adataink folyamatos használatban és mozgásban

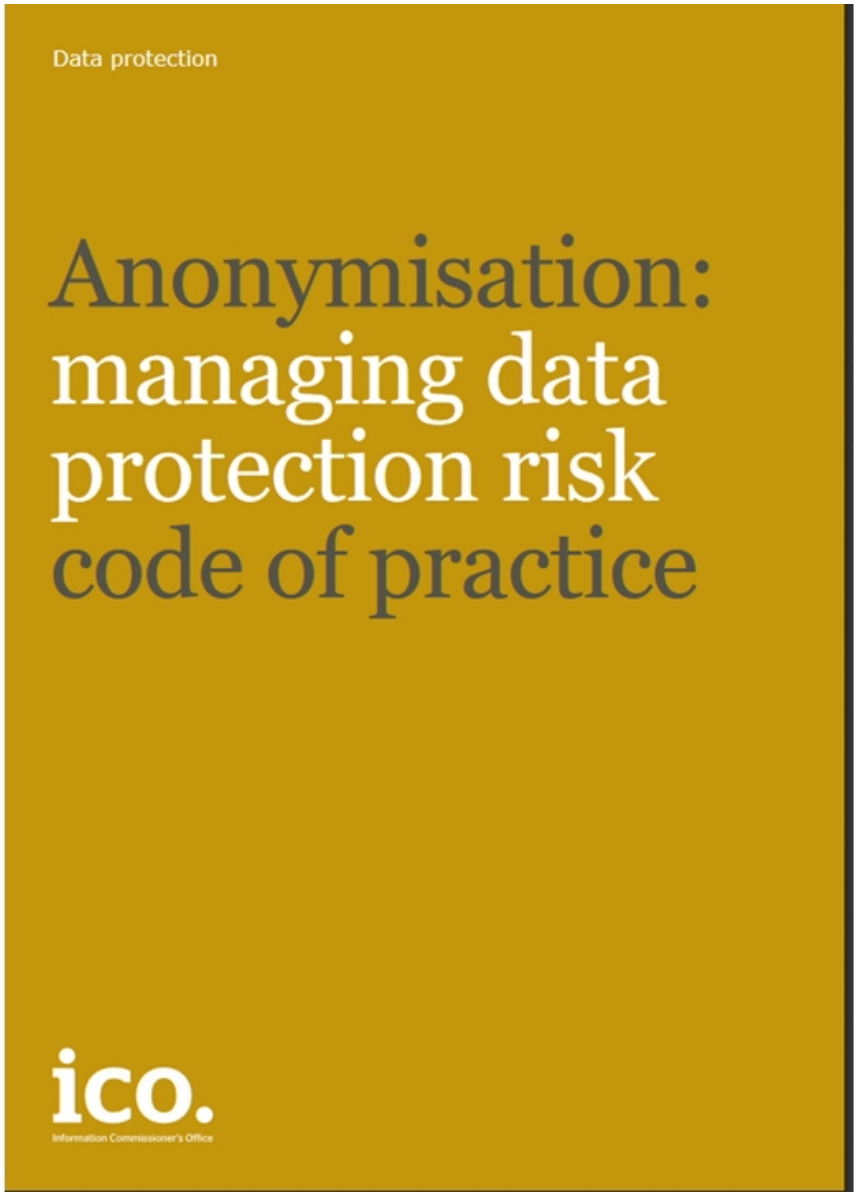


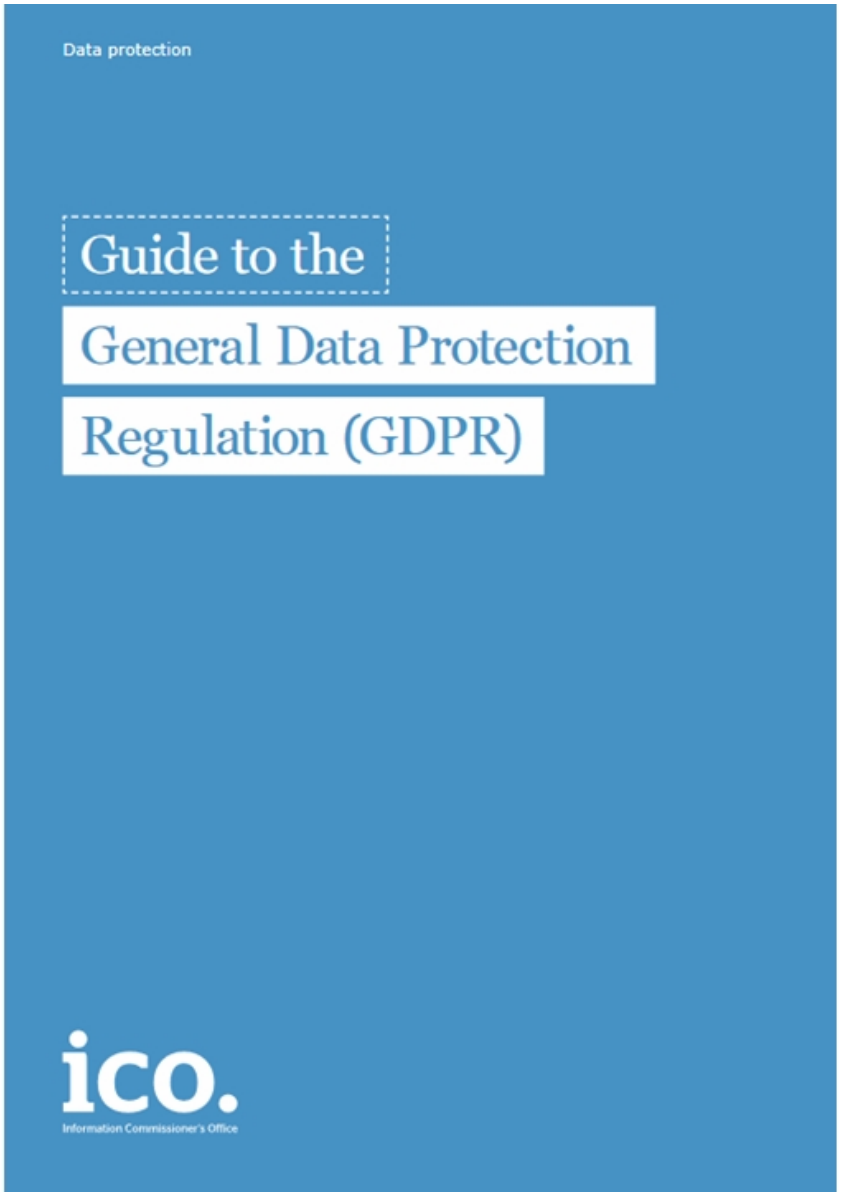
Adattitkosítás – felhasználási területek

1. Kockázatok mérséklése Személyazonosítási adatokat (PII), Védett egészségügyi adatokat (PHI) és Pénzügyi adatokat (PCI) kezelő rendszerekben
2. Big data elemzésekhez, illetve tesztelésekhez adatok biztosítása az érzékeny adatok kiadása nélkül
3. Felhőbe átmozgatott szolgáltatások adatvédelme (IaaS, PaaS)
4. Törvényi szabályzások, Megfelelőség: PCI, HIPAA, GDPR
5. Hatókör csökkentés (szabályozásoknál)
6. Titkosítás végponttól végpontig (érzékeny/pénzügyi adatok)

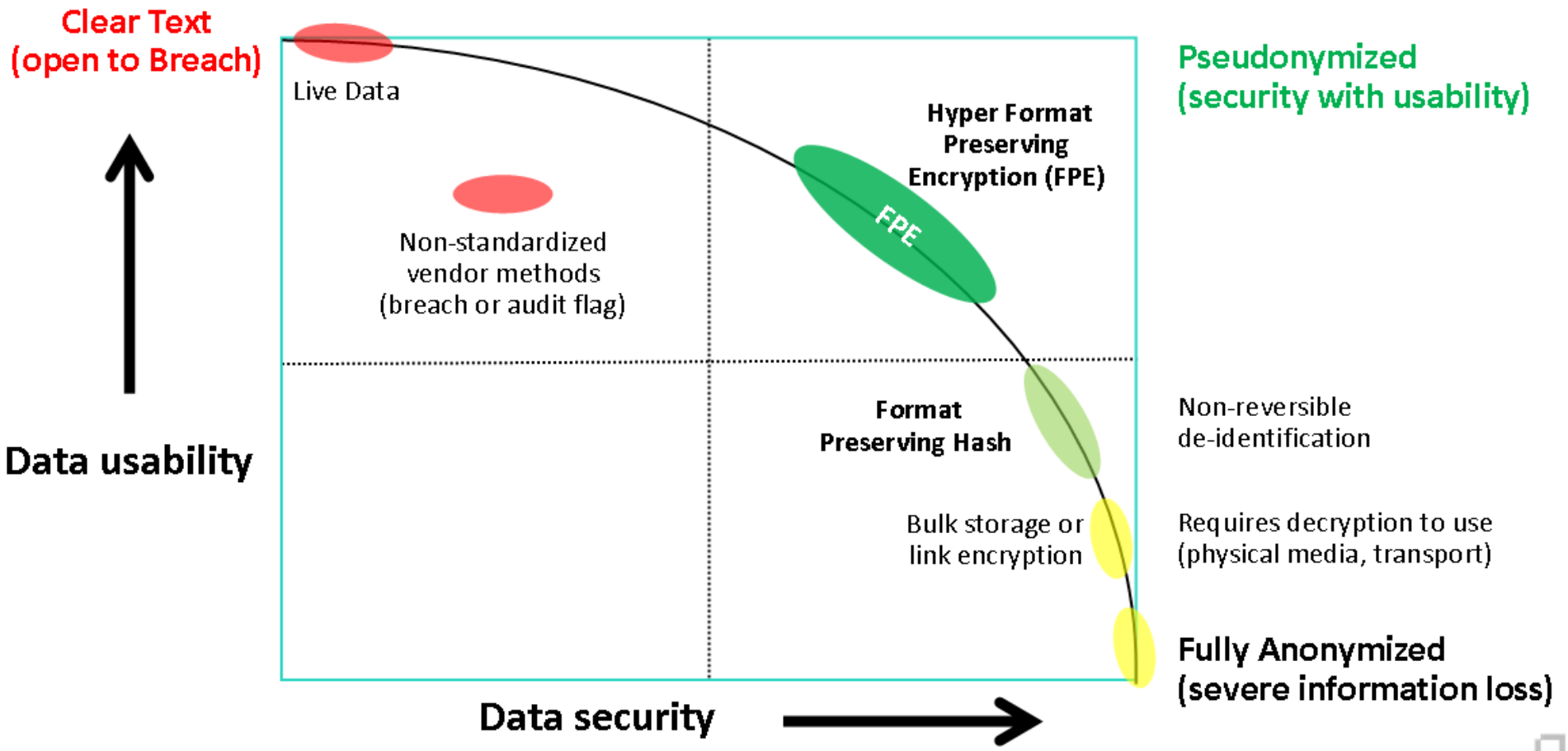
GDPR
32. cikk - Az adatkezelés biztonsága

- (1) Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:
- a) a személyes adatok álnevesítését és titkosítását;


Data protection
Anonymisation: managing data protection risk code of practice
ico.
Information Commissioner's Office


Data protection
Guide to the General Data Protection Regulation (GDPR)
ico.
Information Commissioner's Office

Titkosítási technológiák



Format-Preserving Encryption (FPE)

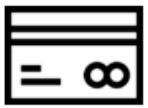
Vezetéknév: Tátrai
Keresztnév: Levente
SSZ: 934-72-2356
SZI: 08-07-1966

Vezetéknév: Máltai
Keresztnév: Adorján
Ügyfélazonosító: 122105278 674301068

AES-FPE	**Vezetéknév: Uywjlq Keresztnév: Muwruwwb** SSZ: **253- 67**- 2356 **SZI**: **01-02-1972**	**Vezetéknév: KxýAçy Keresztnév: ĎwläÜqß** Ügyfélazonosító: 122105278 **827572346**
AES-CBC	**Vezetéknév:** OGIJNzUJNTUJNGEJNDUJNWYJYmUJNjcJNDkJNjgJMjIJYWIJN2MJMjEJN2UJMzMNCg== ...	**Vezetéknév:** NDggMzQgMTAgNWIgYzcgMTIgYTYgZjggMTcgM2UgZWQgOTEgMzIgNzcgNmQgNzI= ...

- Sokféle adattípus és formátum támogatott: név, lakcím, dátum, számsor, sorozatszám, stb.
- Unicode karakterkészletek támogatása (Magyar nyelv)
- Biztosít integritásvédelmet (referenciális)
- Leginkább éles környezetek védelmére és adatmaszkolásnál használatos

Secure Stateless Tokenization (SST)



Bankkártya

4171 5678 8765 4321

SST	**8736 5533 4678 9453**
Részleges SST	4171 56**33 4678** 4321
Egyszerű SST	4171 56**AZ UYTZ** 4321
BIN Mapping	**12**36 56**33 4678** 4321

Hatalmas
Token Tárak

120 MB RAM
SST Mapping
Tábla

- Token adatbázis helyett pehelysúlyú token mapping tábla
- Token értékek megfeleltetése véletlen számokkal
- Meghatározóan kisebb költség
  - Nem kell adatbázishoz sem hw, sem sw, nincs replikációs hiba vagy karbantartás…

Adatok védeleme FPE és SST szolgáltatásokkal

Name	SS#	Credit Card #	Street Address	Customer ID
James Potter	385-12-1199	3712 3456 7890 1001	1279 Farland Avenue	G8199143
Ryan Johnson	857-64-4190	5587 0806 2212 0139	111 Grant Street	S3626248
Carrie Young	761-58-6733	5348 9261 0695 2829	4513 Cambridge Court	B0191348
Brent Warner	604-41-6687	4929 4358 7398 4379	1984 Middleville Road	G8888767
Anna Berman	416-03-4226	4556 2525 1285 1830	2893 Hamilton Drive	S9298273

FPE FPE SST FPE FPE

Name	SS#	Credit Card #	Street Address	Customer ID
Kwfdv Cqvzgk	161-82-1292	3712 3486 3545 1001	2890 Ykzbpoi Clpppn	S7202483
Veks Iounrfo	200-79-7127	5587 0856 7634 0139	406 Cmxto Osfalu	B0928254
Pdnme Wntob	095-52-8683	5348 9209 2367 2829	1498 Zejojtbbx Pqkag	G7265029
Eskfw Gzhqlv	178-17-8353	4929 4333 0934 4379	8261 Saicbmeayqw Yotv	G3951257
Jsfk Tbluhm	525-25-2125	4556 2545 6223 1830	8412 Wbbhalhs Ueyzg	B6625294

Biztonságos adathozzáférés szigorú szabályzásnak megfelelően

Name	SS#	Credit Card #	Street Address	Customer ID
Anna Berman	416-03-4226	4556 2525 1285 1830	2893 Hamilton Drive	S9298273

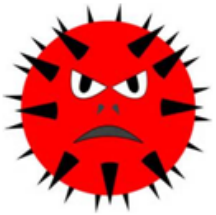
- Garantált integritású adat vagy teljesen randomizált kimenet szabályzástól függően
- Igény szerint védett vagy azonosíthatatlan adat egyetlen keretrendszerből
  - Felhasználható teszt adatok generálására a minőségbiztosításhoz vagy prezentációkhoz, oktatásokhoz.

Adatcentrikus védelem nélkül

HR Rendszer

ETL Eszközök

Mainframe Alkalmazás



Malware

Name	SS#	Credit Card #	Street Address	Customer ID	State	Score
James Potter	385-12-1199	3 712 345 678 901 000	1279 Farland Avenue	G8199143	NY	100
Ryan Johnson	857-64-4190	5587 0806 2212 0139	111 Grant Street	S3626248	NY	**200**
Carrie Young	761-58-6733	5348 9261 0695 2829	4513 Cambridge Court	B0191348	CA	120
Brent Warner	604-41-6687	4929 4358 7398 4379	1984 Middleville Road	G8888767	CA	**120**
Anna Berman	416-03-4226	4556 2525 1285 1830	2893 Hamilton Drive	S9298273	KY	160

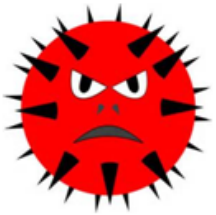
Elemzők

Ügyfélszolgálat

DB Adminisztrátorok

Rosszindulatú Támadó

Titkosítás esetén az adatokat hozzáféréssel is csak kódolt formában láthatják



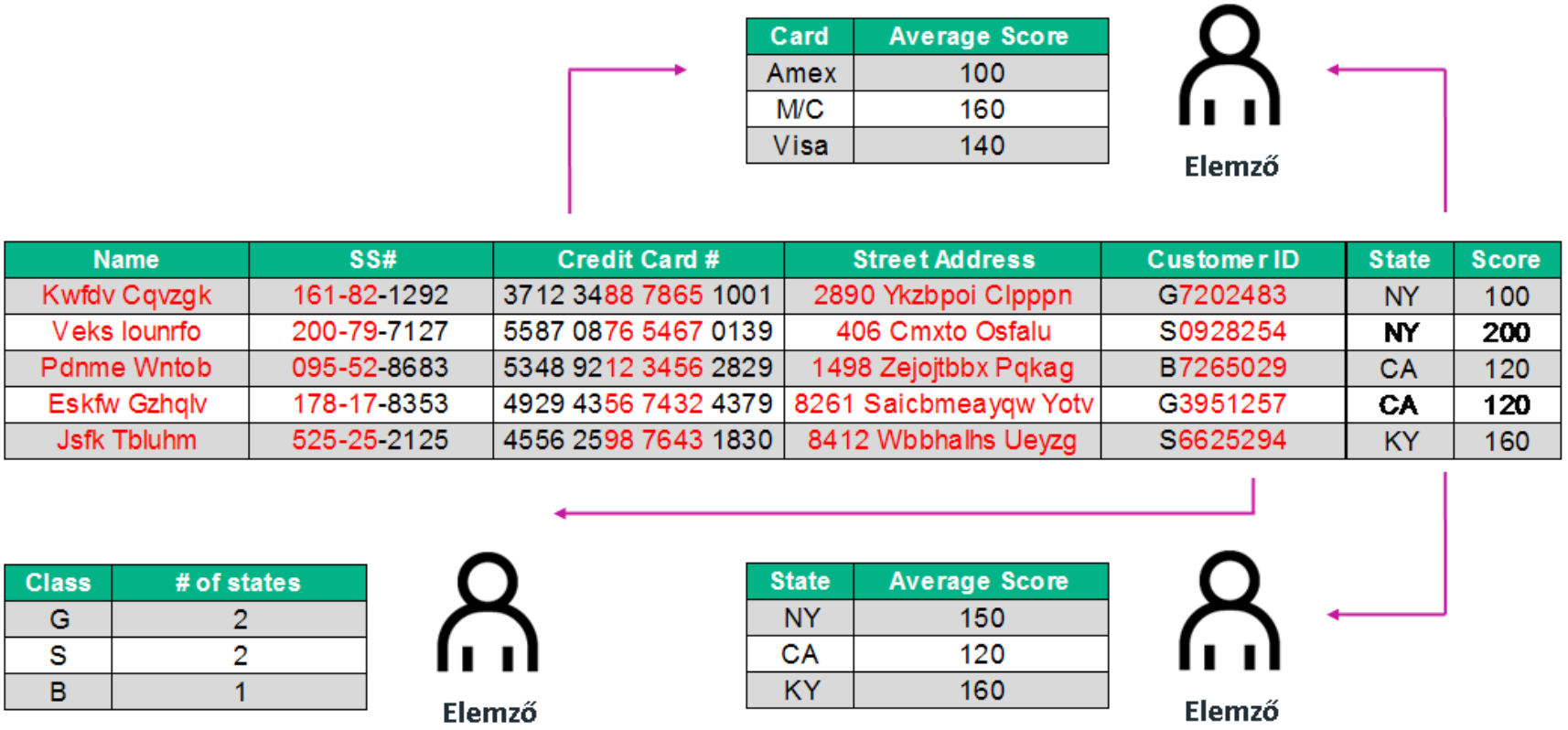
Malware

Name	SS#	Credit Card #	Street Address	Customer ID	State	Score
Kwfdv Cqvzgk	161-82-1292	3712 3488 7865 1001	2890 Ykzbpoi Clpppn	G7202483	NY	100
Veks Iounrfo	200-79-7127	5587 0876 5467 0139	406 Cmxto Osfalu	S0928254	**NY**	**200**
Pdnme Wntob	095-52-8683	5348 9212 3456 2829	1498 Zejojtbbx Pqkag	B7265029	CA	120
Eskfw Gzhqlv	178-17-8353	4929 4356 7432 4379	8261 Saicbmeayqw Yotv	G3951257	**CA**	**120**
Jsfk Tbluhm	525-25-2125	4556 2598 7643 1830	8412 Wbbhalhs Ueyzg	S6625294	KY	160

DB Adminisztrátorok

Rosszindulatú Támadó

Statisztikai elemzések maszkolt adatokkal is végezhetőek



Részlegesen maszkolt adatok adott alkalmazások számára

Fizetési alkalmazás

Name	SS#	Credit Card #	Street Address	Customer ID	State	Score
Kwfdv Cqvzgk	161-82-1292	3712 3488 7865 1001	2890 Ykzbpoi Clpppn	G7202483	NY	100
Veks lounrfo	200-79-7127	5587 0876 5467 0139	406 Cmxto Osfalu	S0928254	**NY**	**200**
Pdnme Wntob	095-52-8683	5348 9212 3456 2829	1498 Zejojtbbx Pqkag	B7265029	CA	120
Eskfw Gzhqlv	178-17-8353	4929 4356 7432 4379	8261 Saicbmeayqw Yotv	G3951257	**CA**	**120**
Jsfk Tbluhm	525-25-2125	4556 2598 7643 1830	8412 Wbbhalhs Ueyzg	S6625294	KY	160

Ügyfélszolgálat

Autorizált alkalmazások számára valódi adatok elérése

Autorizált HR Alkalmazás

Voltage SecureData Eszközök

Name
James Potter
Ryan Johnson
Carrie Young
Brent Warner
Anna Berman

Name	SS#	Credit Card #	Street Address	Customer ID	State	Score
Kwfdv Cqvzgk	161-82-1292	3712 3488 7865 1001	2890 Ykzbpoi Clpppn	G7202483	NY	100
Veks lounrfo	200-79-7127	5587 0876 5467 0139	406 Cmxto Osfalu	S0928254	**NY**	**200**
Pdnme Wntob	095-52-8683	5348 9212 3456 2829	1498 Zejojtbbx Pqkag	B7265029	CA	120
Eskfw Gzhqlv	178-17-8353	4929 4356 7432 4379	8261 Saicbmeayqw Yotv	G3951257	**CA**	**120**
Jsfk Tbluhm	525-25-2125	4556 2598 7643 1830	8412 Wbbhalhs Ueyzg	S6625294	KY	160

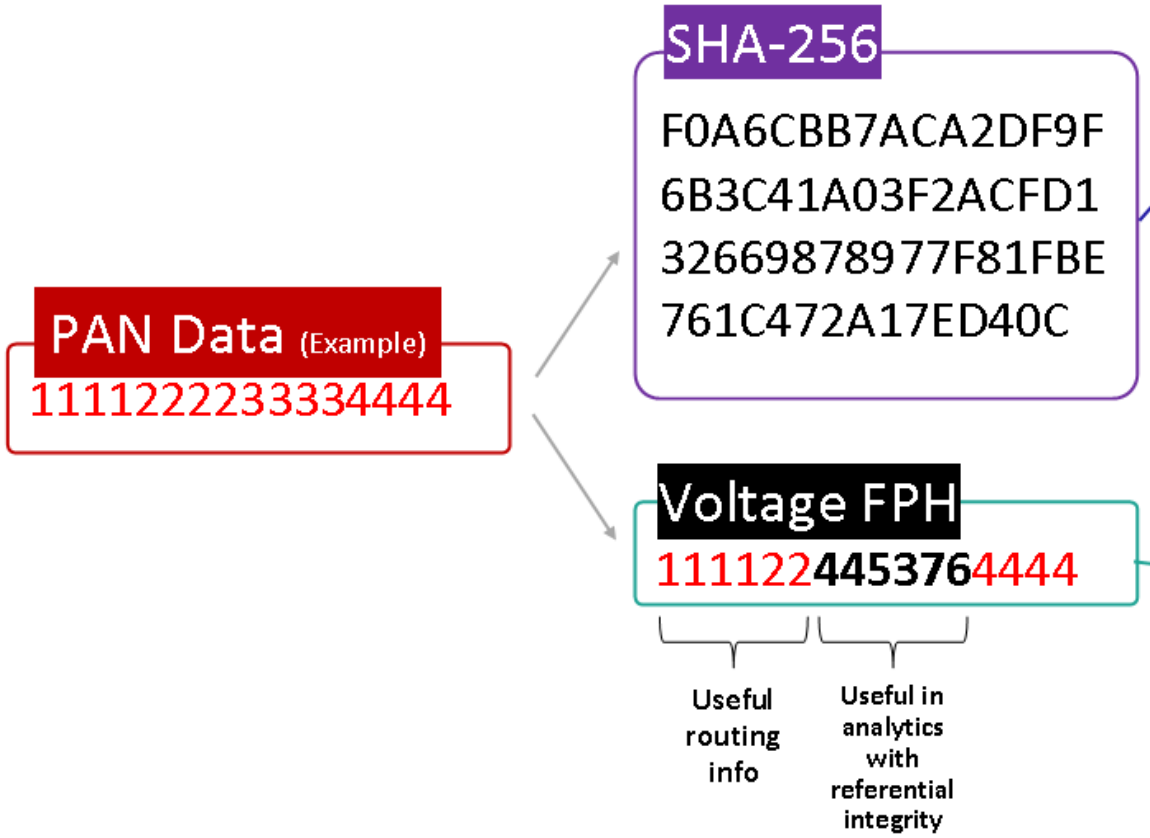
Autorizált Elemző

Voltage SecureData Eszközök

SS#
385-12-1292
857-64-7127
761-58-8683
604-41-8353
416-03-2125

Anonymization: Format-preserving hash

One-way transformation for privacy compliance and other use cases

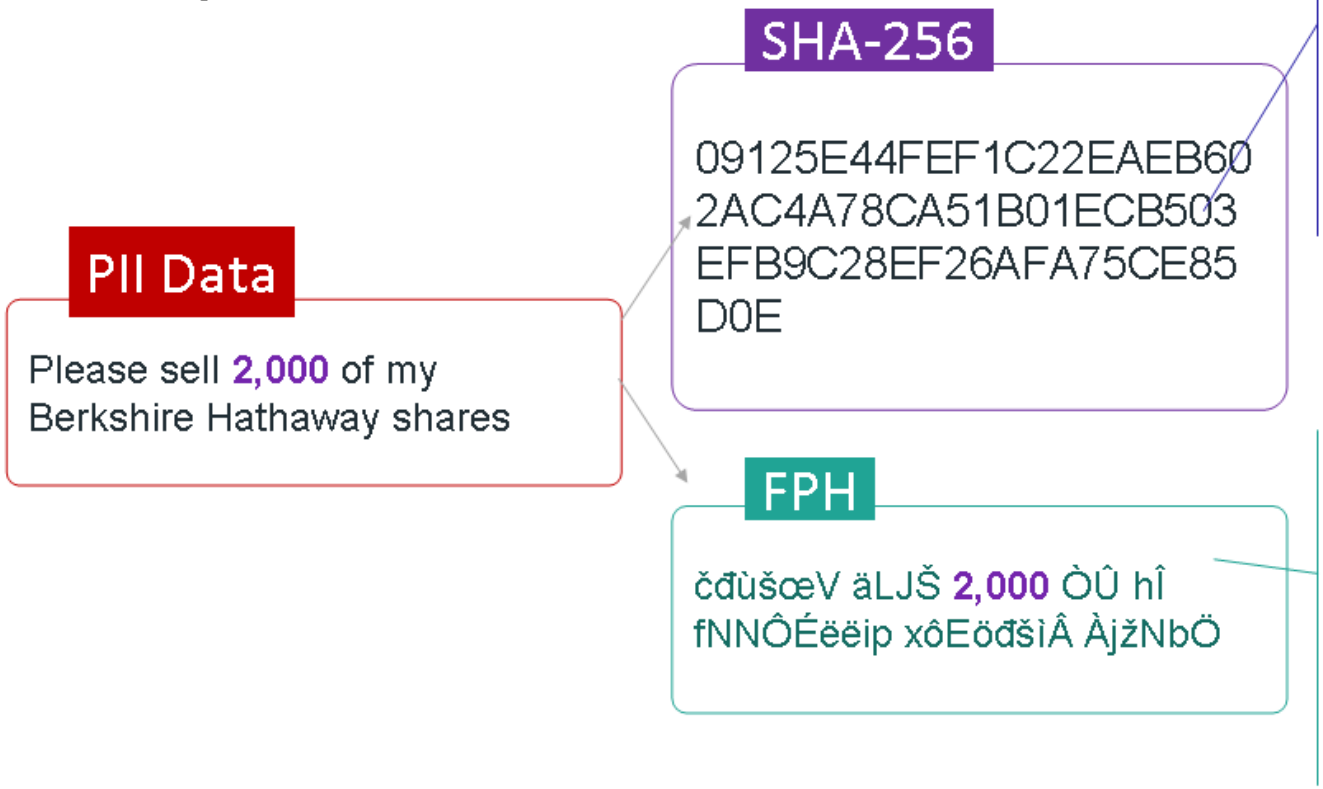


- Requires DB schema changes
- Breaks apps and middleware
- Does not allow partial hash
- Cannot preserve length or relationships

- One-way transformation
- Strength of FPE applied
- Works with existing DB schemas and applications—no changes
- Non-reversible yet can be used in analytics to de-identify data
- Maintain lengths and partial hash

Format-Preserving Hash vs. Hash

Example 2

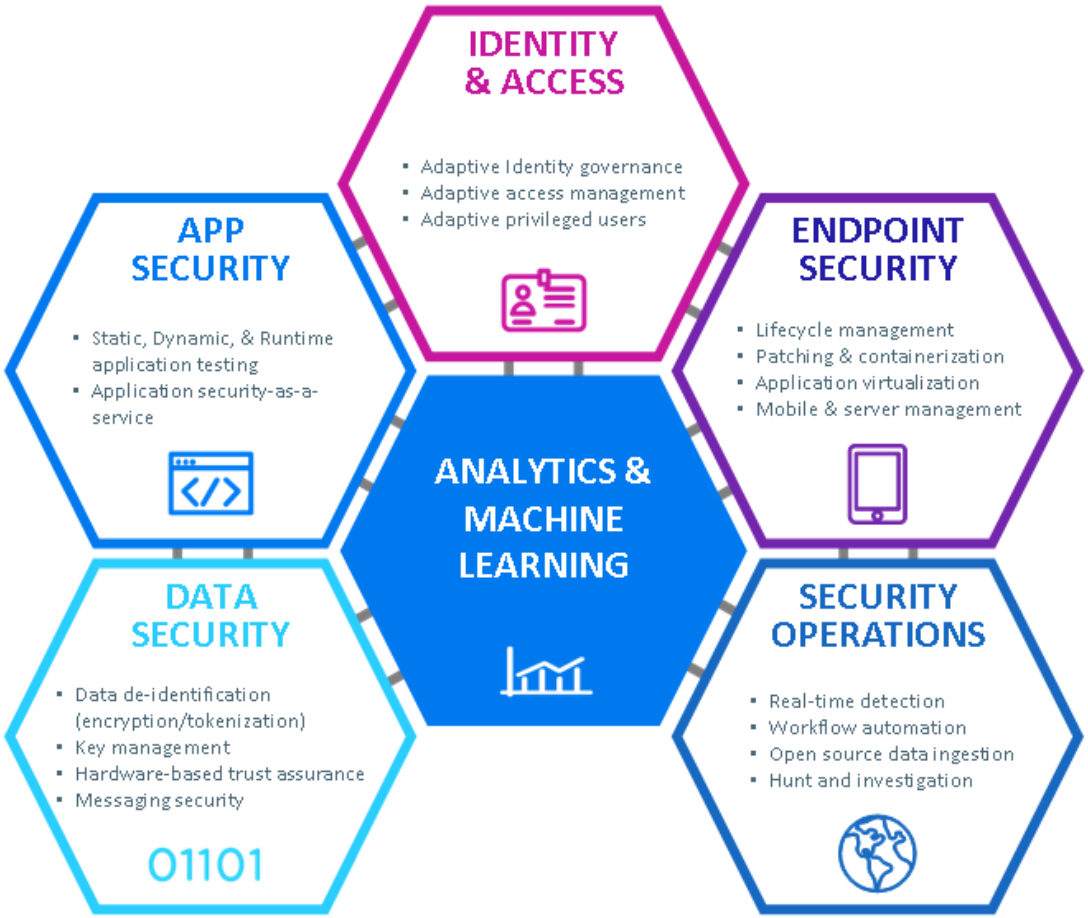


- Requires changes to DB schemas
- Breaks applications and middleware
- Does not allow partial hash
- Cannot preserve length or relationships

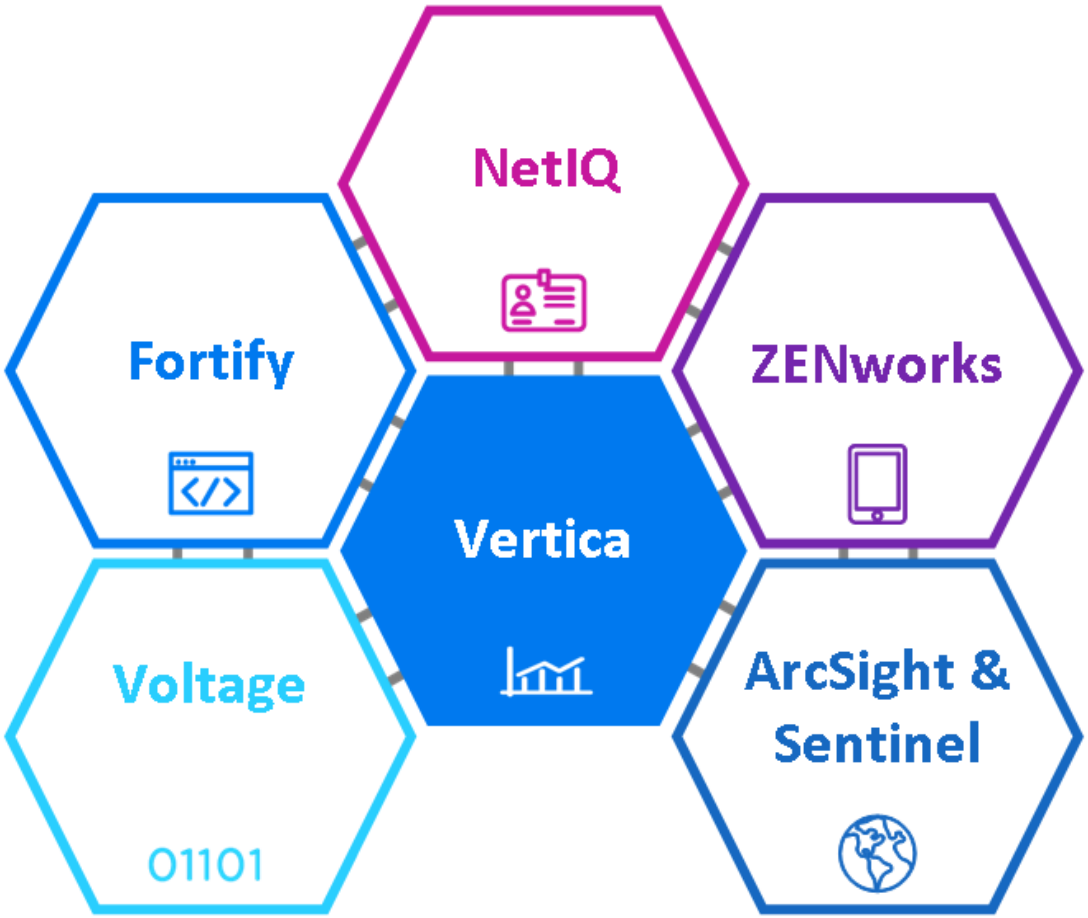
- Works with existing DB schemas and application
- Non-reversible yet can be used in **analytics**
- Maintain length, or partial hash
- GDPR Article 17 'Right to Erasure'

Comprehensive security for the enterprise

Comprehensive security for the enterprise



MICRO FOCUS®
Security



Köszönöm a figyelmet!

www.microfocus.com/solutions/security