Microsoft

Az új kiberfenyegetések kora

Az elmúlt év tanulságai

Liebhardt Péter
Cybersecurity Architect

A kiberbűnözés állapota

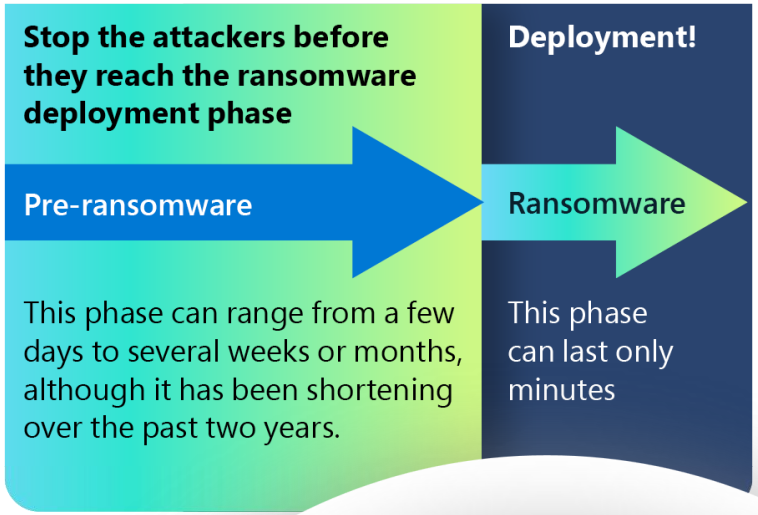
Amint a kibervédelem fejlődik és egyre több szervezet választja a proaktív megközelítést a megelőzés terén, a támadók alkalmazkodnak technikáikhoz

Ransomware állapota

Ember által működtetett ransomware célzási és sikerarány modell

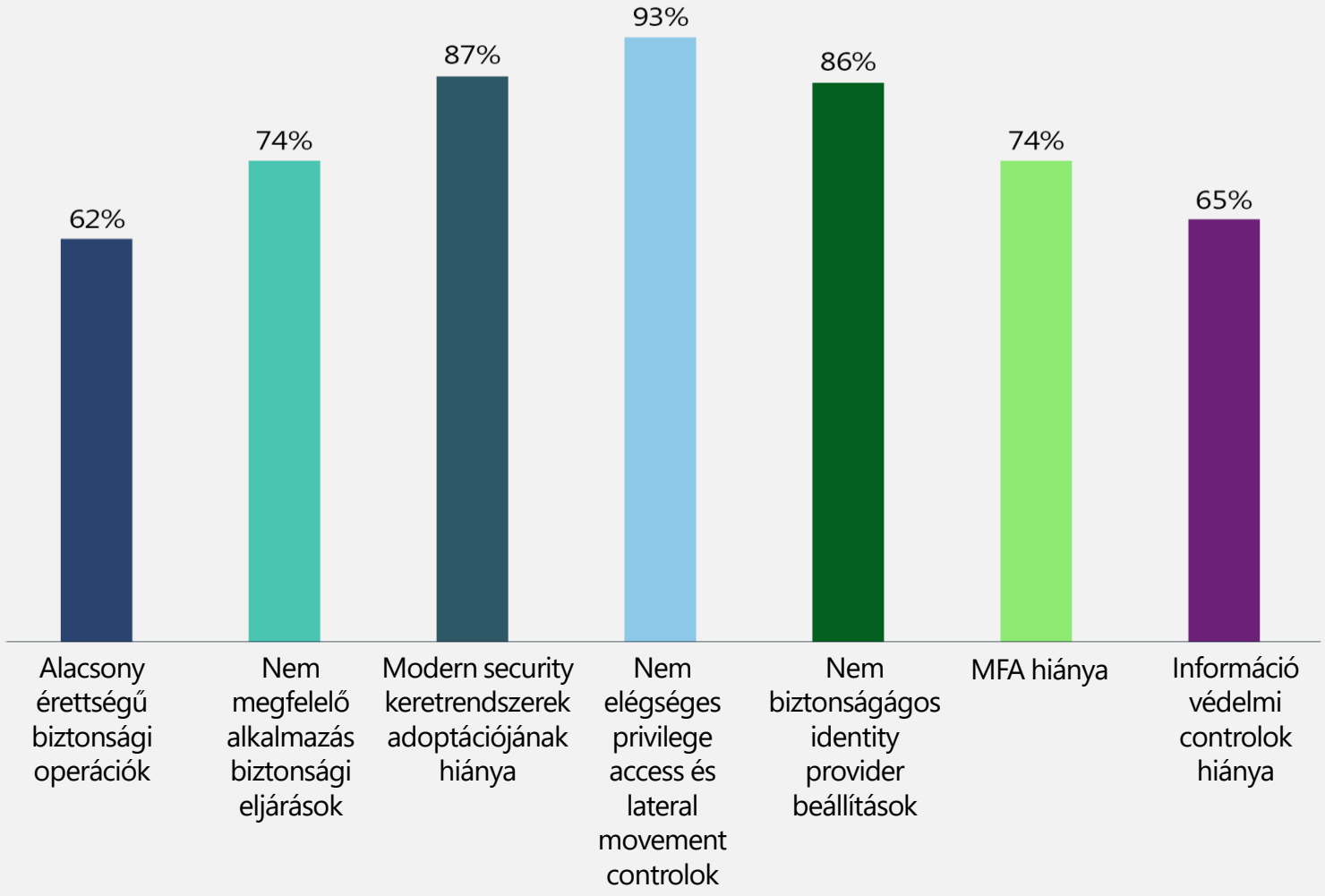
Microsoft Defender for Endpoint (EDR) adatai alapján

Az átlagos ember által végrehajtott támadás

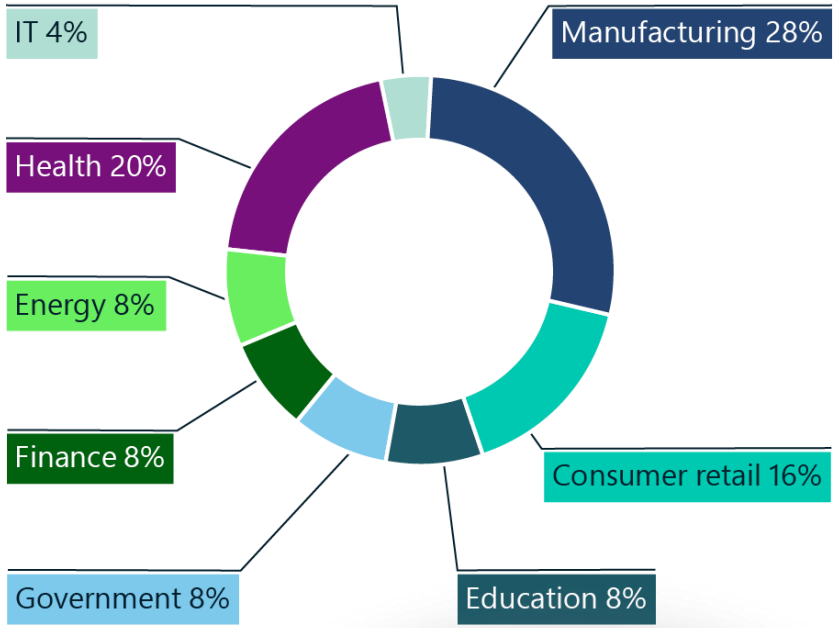


A támadóknak inkább hitelesítő adatokra van szükségük műveleteik sikeréhez, mint a rosszindulatú szoftverekre. Egy egész szervezetet érintő, sikeres emberi irányítású zsarolóvírus-fertőzés alapvetően egy magasan privilegizált fiókhoz való hozzáférésen múlik.

Ransomware tapasztalatok



Ransomware incidensek és helyreállítási projektek ágazatonként



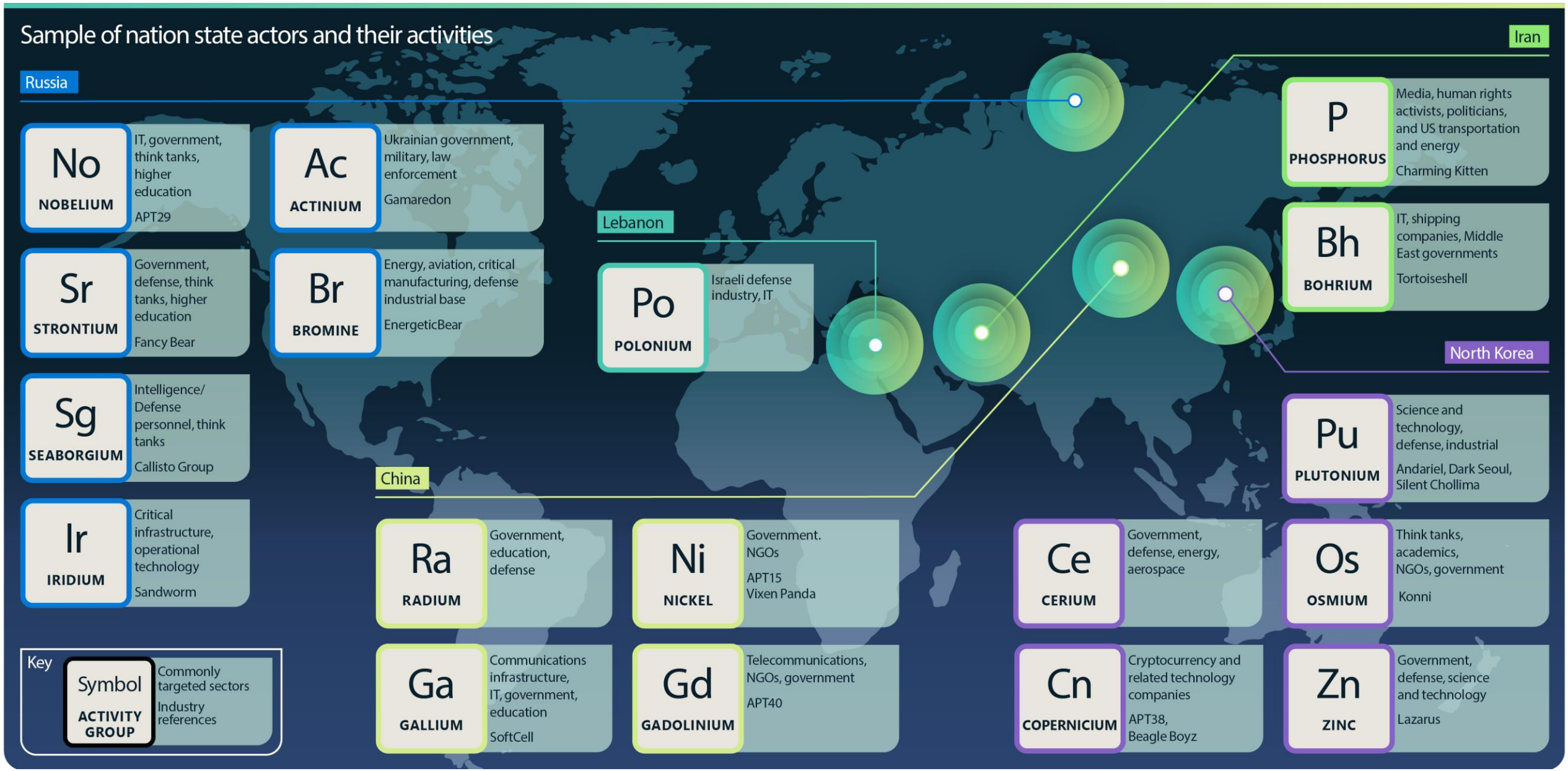
93%

a Microsoft ransomware helyreállítási vizsgálatainak kimutatta, hogy nem elégségesek a privilege access és lateral movement controlok.

Nemzetállamokhoz köthető fenyegetések

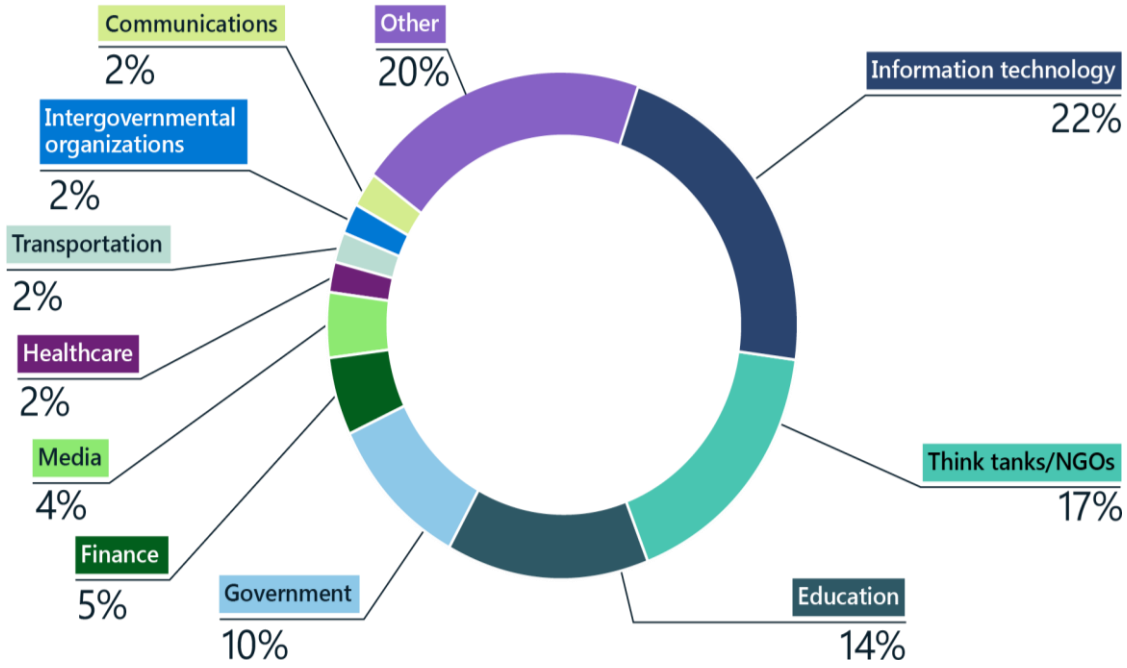
Az állami szereplők egyre kifinomultabb kibertámadásokat indítanak, hogy elkerüljék a felfedezést és további stratégiai prioritásaikat előmozdítsák.

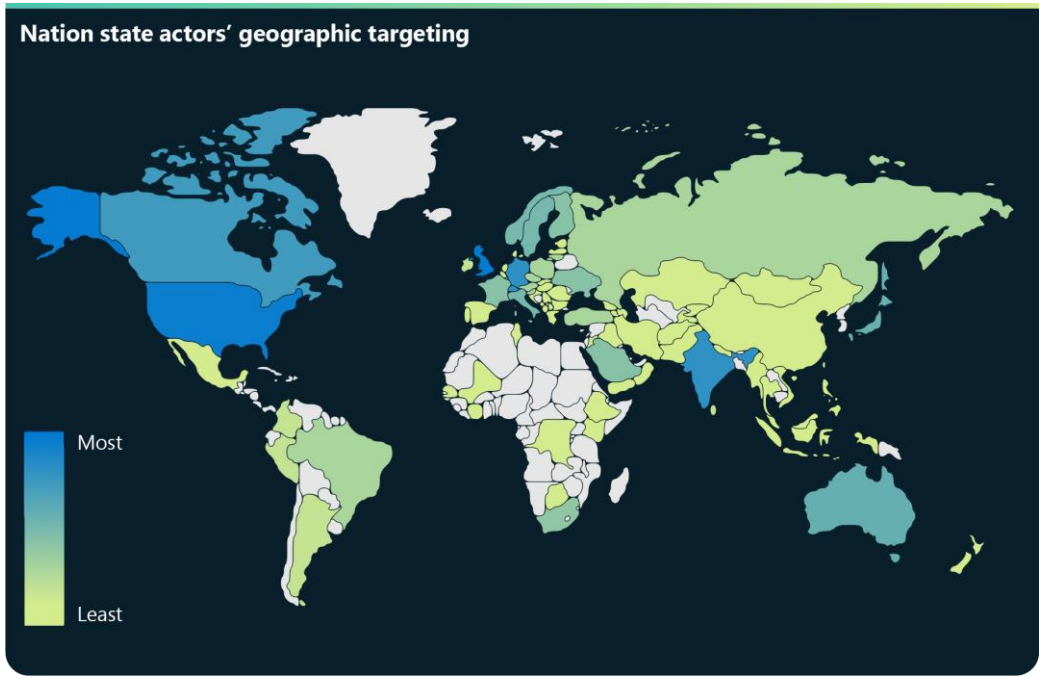
About our nation state data



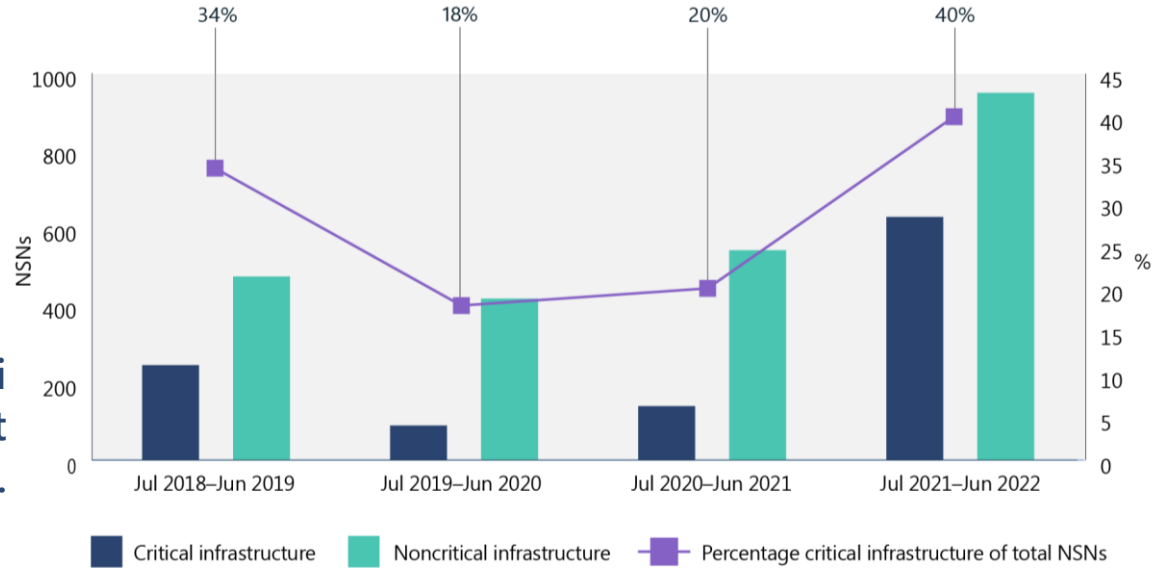
Az állandóan változó fenyegetési környezet

Állami szereplők által célozott iparági szektorok

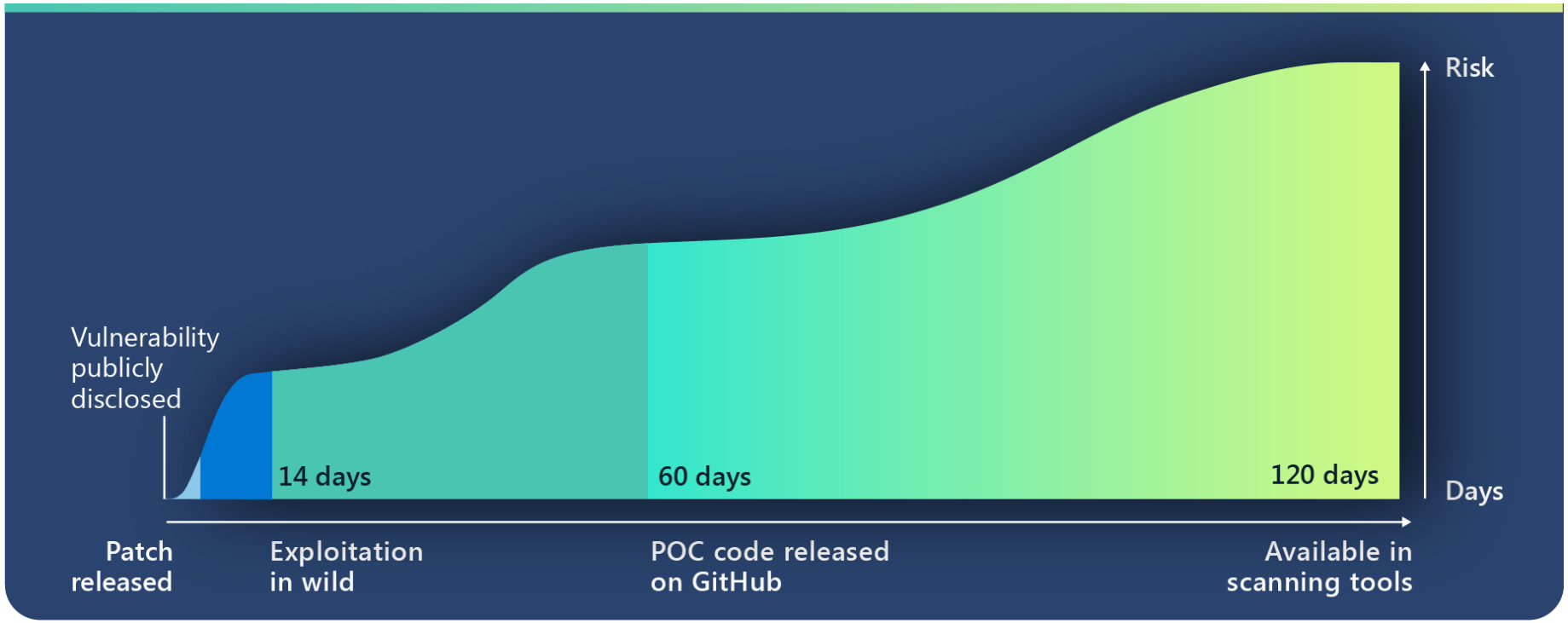




Az elmúlt évben megnőtt az állami szereplők általi kritikus infrastruktúrát célzó támadások aránya.



A sebezhetőségek gyors kihasználása

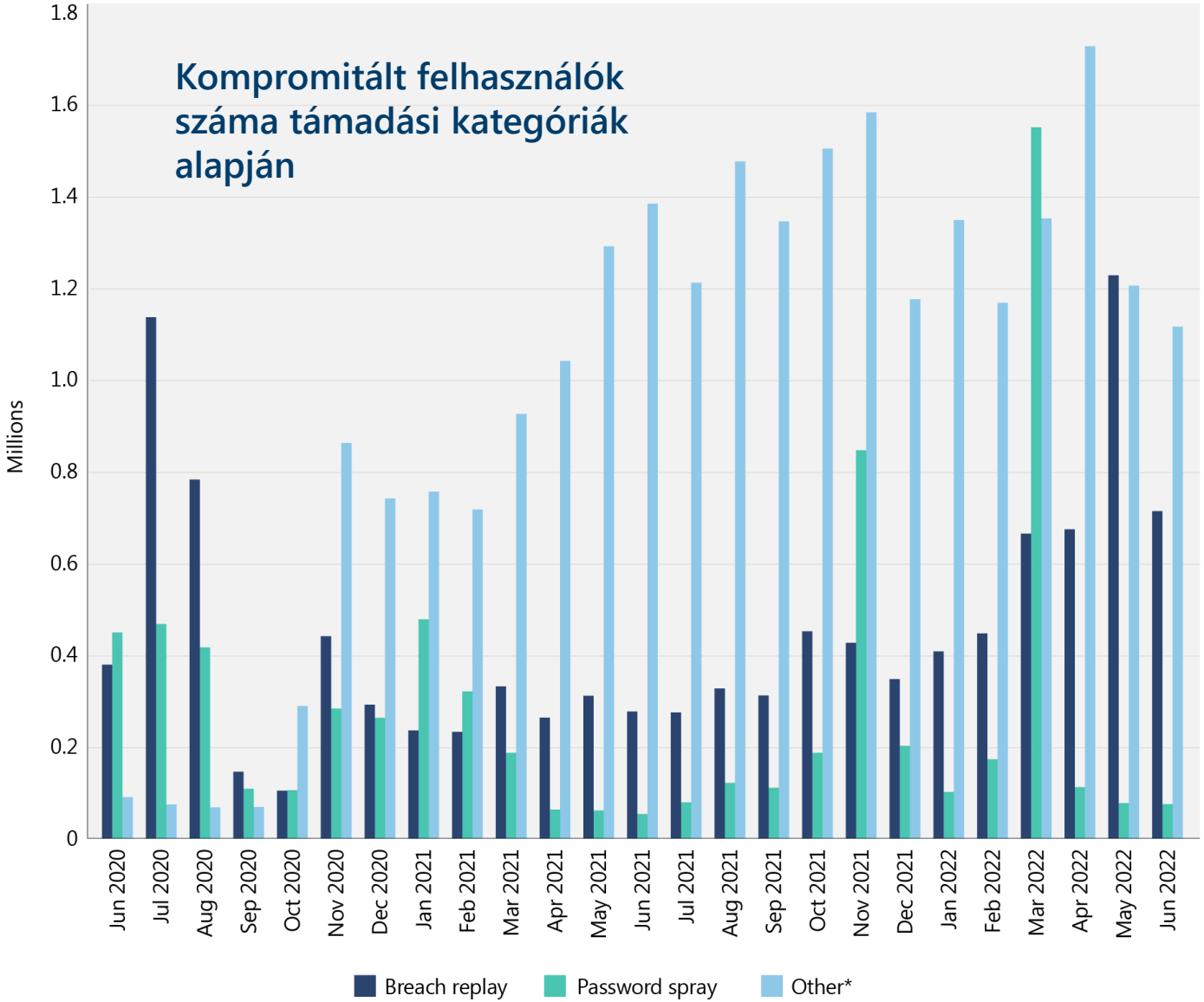


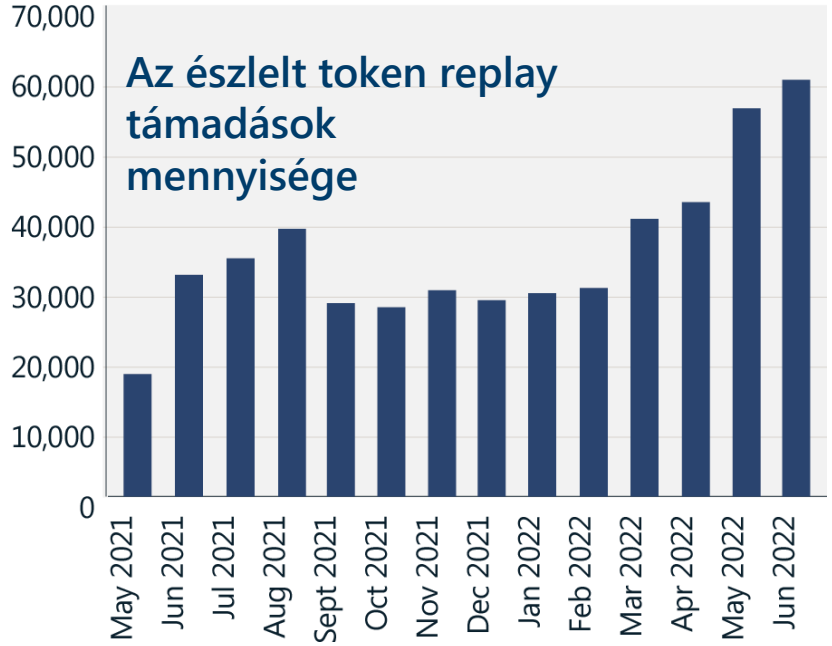
A sebezhetőség árucikké tételének sebessége és mértéke

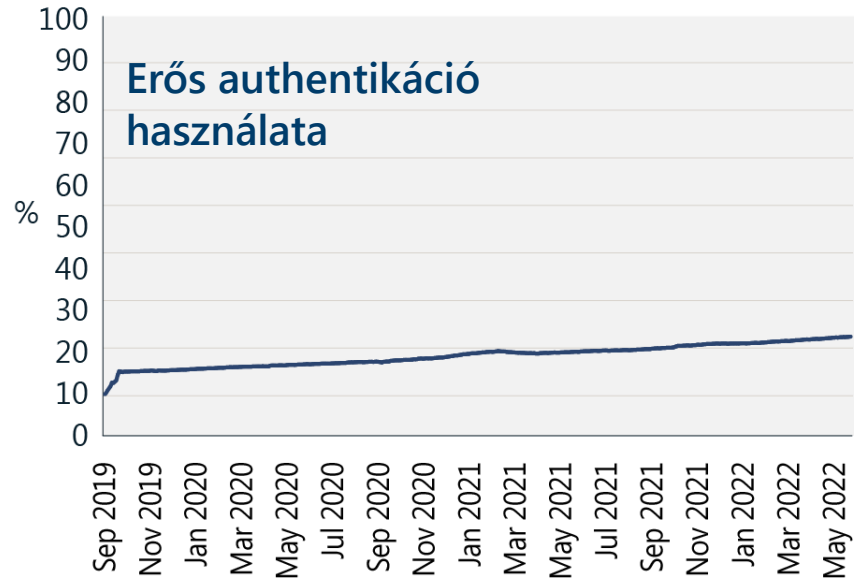
Cyber Resilience

A modernizáció kockázatainak és előnyeinek megértése meghatározó fontosságú

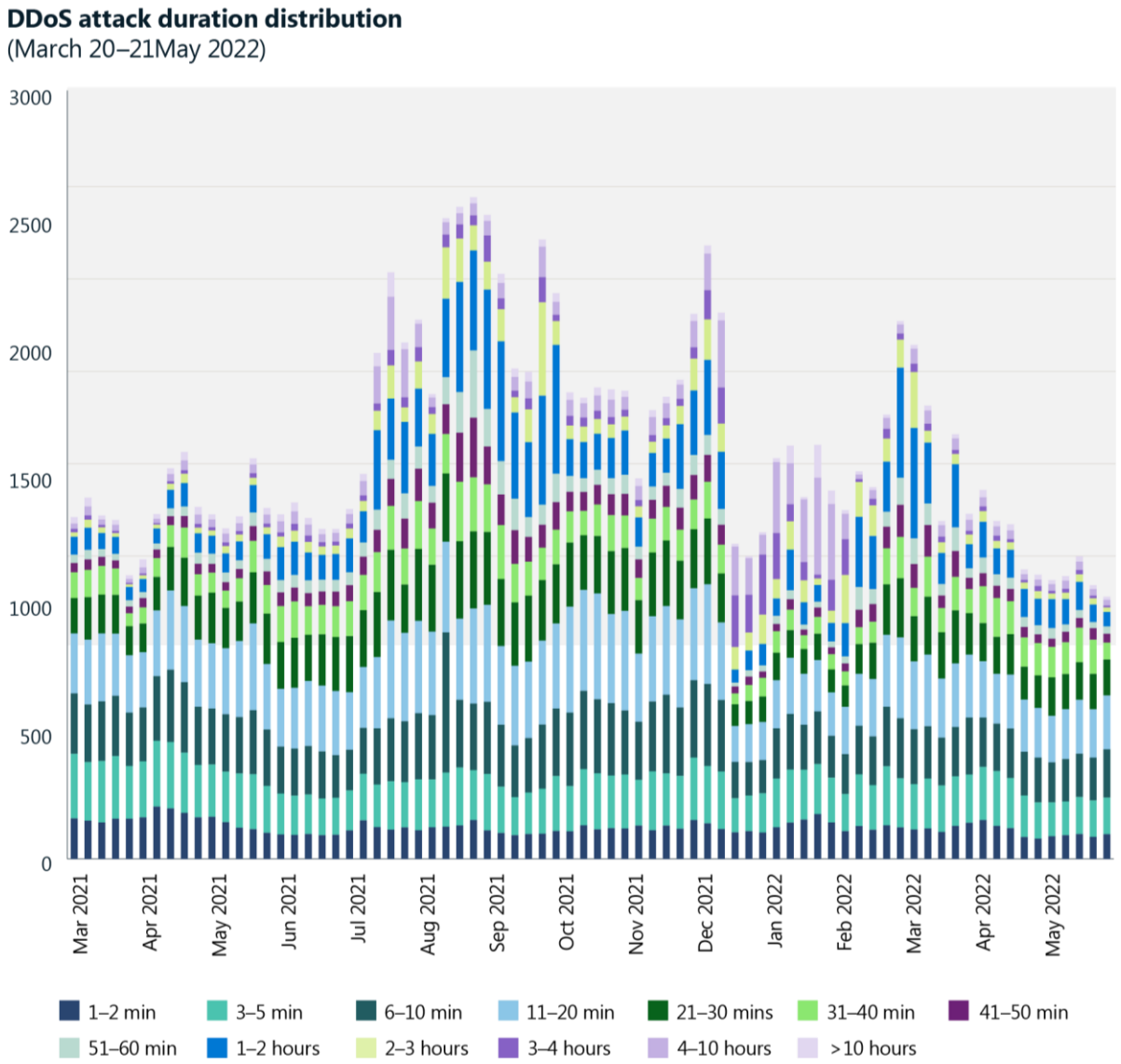
Identity

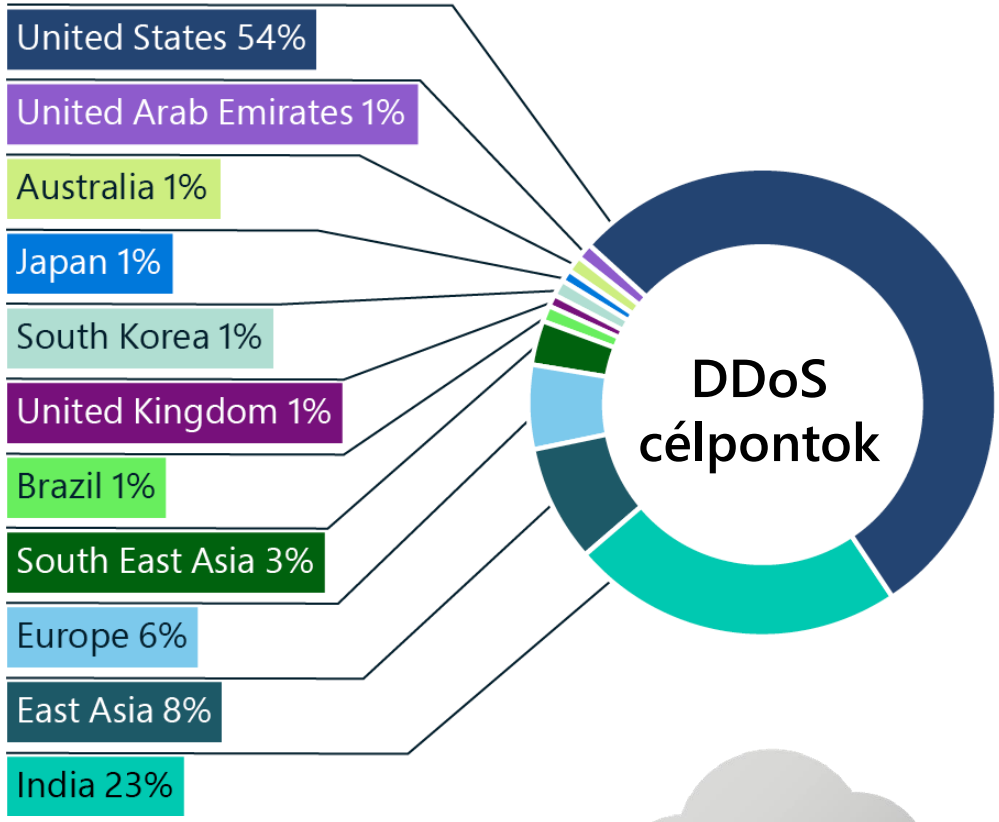

Kompromitált felhasználók száma támadási kategóriák alapján
Millions
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0
Jun 2020
Jul 2020
Aug 2020
Sep 2020
Oct 2020
Nov 2020
Dec 2020
Jan 2021
Feb 2021
Mar 2021
Apr 2021
May 2021
Jun 2021
Jul 2021
Aug 2021
Sep 2021
Oct 2021
Nov 2021
Dec 2021
Jan 2022
Feb 2022
Mar 2022
Apr 2022
May 2022
Jun 2022
Breach replay
Password spray
Other*

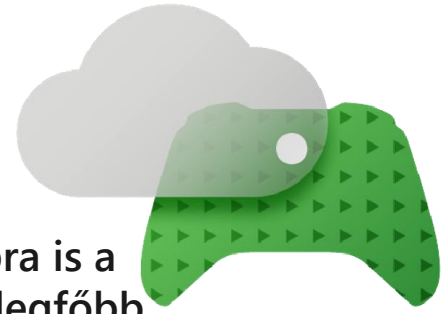

Az észlelt token replay támadások mennyisége
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
May 2021
Jun 2021
Jul 2021
Aug 2021
Sept 2021
Oct 2021
Nov 2021
Dec 2021
Jan 2022
Feb 2022
Mar 2022
Apr 2022
May 2022
Jun 2022


Erős authentikáció használata
%
100
90
80
70
60
50
40
30
20
10
0
Sep 2019
Nov 2019
Jan 2020
Mar 2020
May 2020
Jul 2020
Sep 2020
Nov 2020
Jan 2021
Mar 2021
May 2021
Jul 2021
Sep 2021
Nov 2021
Jan 2022
Mar 2022
May 2022

Mit látunk DDoS oldalon?







A játékipar továbbra is a DDoS támadások legfőbb célpontja.

The cyber resilience bell curve

Minden orgazniáció számára javasolt lépések:

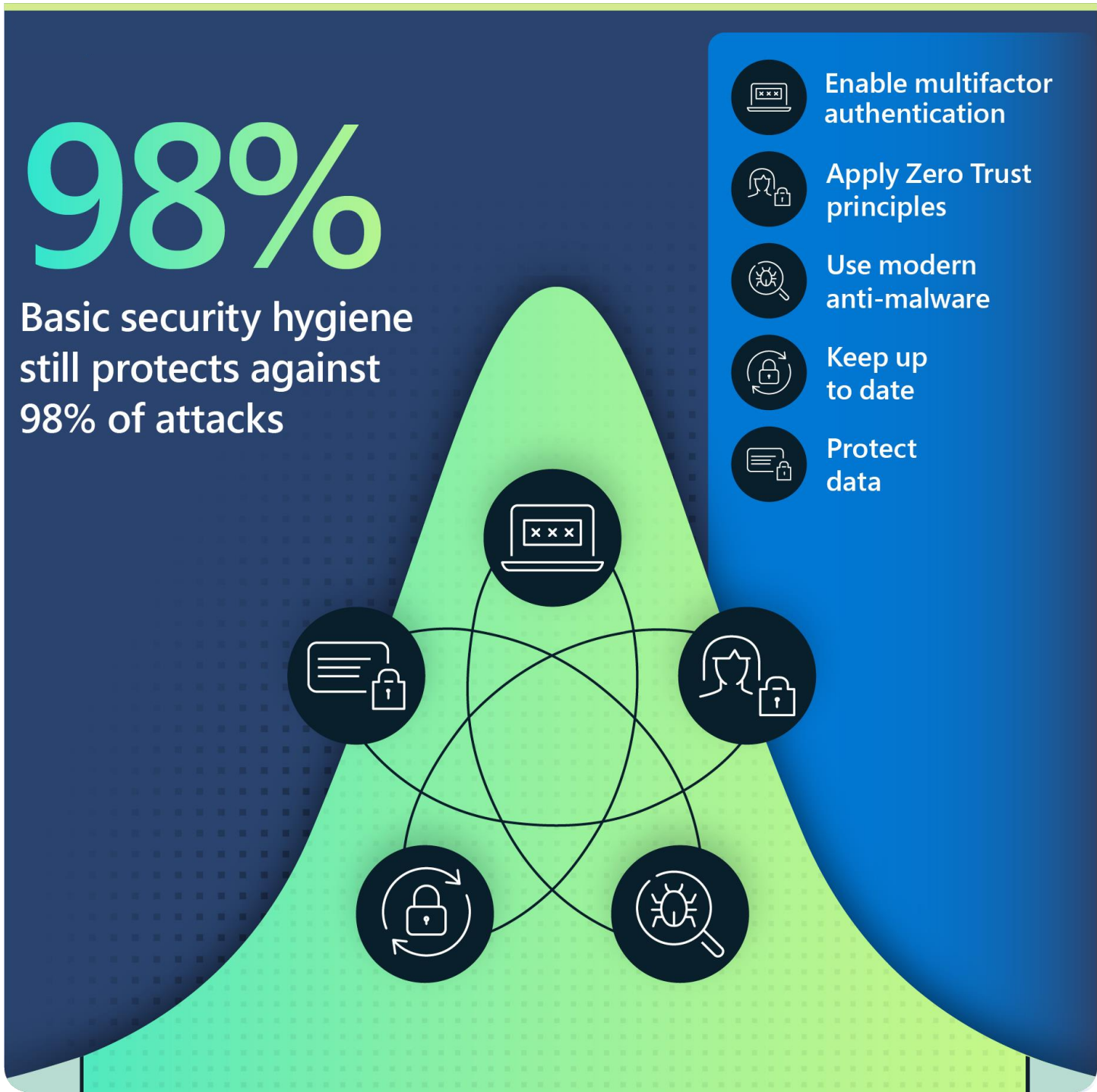
-Multifactor Authentication (MFA)

-Zero Trust

-Modern Anti-Malware / EDR

-Patching (Hardver / Szoftver)

-Data Protection (Backup)



Microsoft

Köszönöm a figyelmet!

- Learn more: https://microsoft.com/mddr
- Dive deeper: https://blogs.microsoft.com/on-the-issues/
- Stay connected: @msftissues and @msftsecurity