
A számítógépes vírusokról

Mi a számítógépes vírus?

A számítógépes vírusok egyszerű, végrehajtható számítógépes programok.

Miután megfertőz egy fájlt vagy a rendszer más részeit, továbbterjed a szomszédos elemekre is.

Mi a számítógépes vírus?

- Önmagát reprodukálja, azaz szaporodik
- Hagyományos eszközökkel nem látható
- Valamilyen állományhoz kapcsolódik
- Lappangási idejük van
- Többnyire kárt, vagy bosszúságot okoz

A vírusok megfertőzhetik ...

- A **programfájlokat**, az **indítórekordokat** és a makróval rendelkező adatfájlokat
- Az **adatlemezeket** és a számítógépek közötti programátvitelhez használt lemezeket, de csak addig, míg azok nem lesznek írásvédettek
- Az elektronikus levélhez **csatolt fájlokat**, de csak a csatolás előtt

A vírusok nem tudják megfertőzni ...

- A hardvert, a képfájlokat, a makró lehetőség nélküli adatfájlokat és a nem futtatható egyéb szoftverrészeket
- Az írásvédett lemezeket
- A szöveges elektronikus leveleket

A vírusok fajtái

- Közvetlen fertőző
  - fertőzött fájl futtatásakor aktivizálódnak
  - átveszik a rendszer irányítását
  - „tiszta” fájlokat keres, amelyeket megfertőzhet
  - a fertőzött program bezárásakor a vírus abbahagyja a fertőzést

A vírusok fajtái

- Tárrezidensen fertőző
  - aktivizálódása után átveszi a rendszer irányítását
  - magánál tartja a rendszer irányítását és közben folyamatosan terjed, mindaddig, míg a memória nem törlődik, még akkor is, ha a fertőzött programot bezárjuk

Hogyan működik a vírus?

- Időzítés
  - számítógépre kerülése után még várakozik
  - lehet dátum, eltelt idő egy fertőzött program indítása óta, valahányadik elindított program a fertőzés óta

Hogyan működik a vírus?

- Töltet
  - Az időzítő hozza működésbe
  - lehet szándékosan romboló hatású (pl.: OneHalf)
  - lehet jóindulatú (csak egy üzenetet jelenít meg, vagy egy dallamot játszik le (pl.: Boza))

A vírusok típusai

- Programvírusok (állományvírusok)
  - futtatható fájlokat fertőz
- Indítóvírusok (boot-vírusok)
  - az indítórekordot fertőzi meg
- Makróvírusok
  - adatfájlokat fertőz

A vírusok típusai

- Worm-ok, vagy férgek
  - Módosítják az operációs rendszert, gyakran a géppel együtt bootolnak, a hálózatot használva levelekhez csatolt állományként terjednek.
  - A csatolt állomány tartalmazza a vírust, melyet aktivizálva (megnézve), elküldi saját magát címjegyzékünk összes tagjának, vagy személyes adatainkat teszi közzé

A vírusok típusai

- Trojan (trójai program)
  - Nem szaporodik és nem terjed

⇩

NEM VÍRUS !!!

  - Olyan program, amely látszólag hasznos célt szolgál, de valójában a célja a fájlok károsítása, illetve vírusok elhelyezése a számítógépen.

A vírusok típusai

- Wabbit
  - A gép erőforrásait emészti fel. Helyi gépen sokszorozódik.
- Backdoor
  - Lehetővé teszi a számítógéphez való hozzáférést.

A vírusok típusai

- Adware
  - Nemkívánt hirdetéseket jelenít meg.
- Spyware
  - Adatokat gyűjt a gép működéséről és elküldi azokat a felhasználó hozzájárulása nélkül.

A vírusok típusai

- Hoaxok
  - Átverések, kacsák
  - Elektronikus levélben „terjed”
  - Félrevezető információ küldése, majd továbbküldése minél több ismerősnek (pl.: téves vírusriasztás)

Mi is az a Malware?

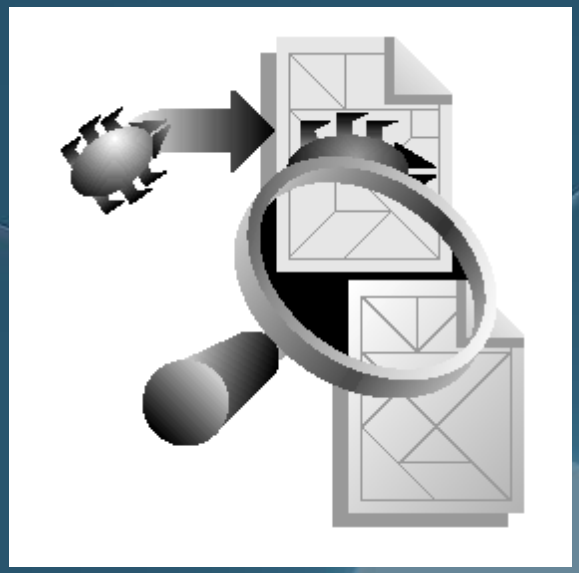
A ***Malware*** egy általános értelmű kifejezés, mely olyan programokra vonatkozik, amelyek pl. hirdetéseket jelenítenek meg, személyes adatokat gyűjtenek, vagy a számítógép konfigurációját állítják át úgy, hogy e tevékenységekbe rendszerint nincs beleszólásunk.

Mi is az a Malware?

Szimptómák:

- Nem kívánt pop-up reklám ablakok nyílnak meg, akkor is ha éppen nem a szörfölünk a weben
- A böngésző kezdő oldala, vagy a beállított kereső motor megváltozik a beleegyezésünk nélkül, ráadásul nem hagyja, hogy visszaállítsuk az eredeti állapotot
- Új és nem kívánt eszköztár jelenik meg a böngészőben, melyet nem lehet leszedni
- Ismeretlen email címekről visszaérkező levelek
- Hirtelen bekövetkező drámai teljesítmény csökkenés
- Az operációs rendszer, a web böngésző, vagy egyéb alkalmazások fagyogatni kezdenek

Vírustechnológiák



- Lopakodó vírusok
  - megpróbálnak elrejtőzni
    - olvasásmegszakítók
    - méretmódosítók

Vírustechnológiák

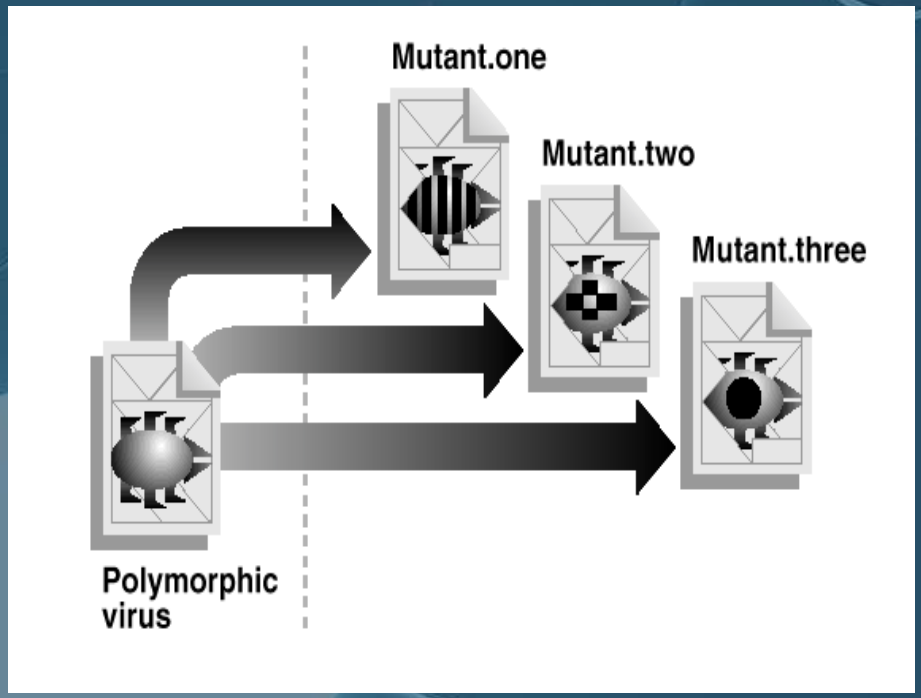
- Önmódosító vírusok
  - mindig módosítja a saját kódját a programtörzsben

    ⇩

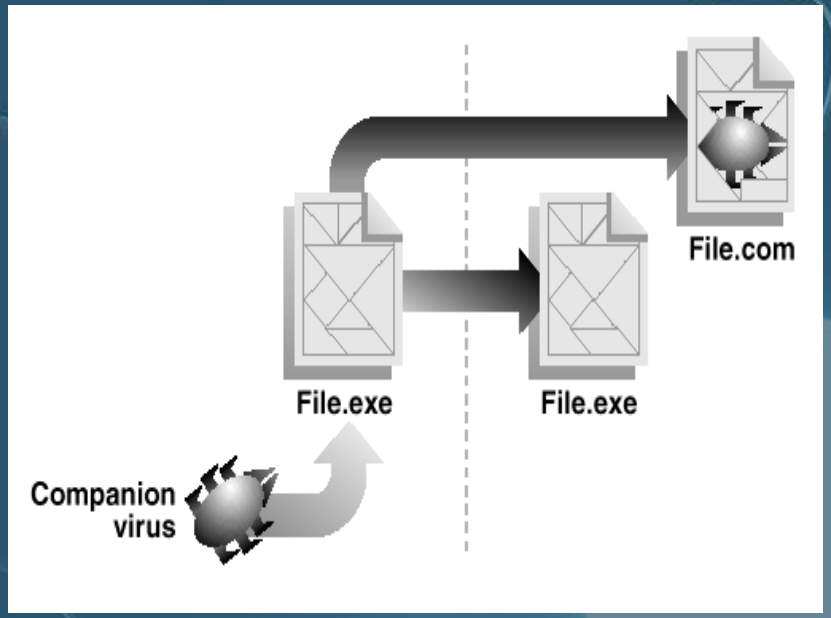
    Nincs két egyforma víruskód.

    ⇩

    Nehezíti az észlelést.



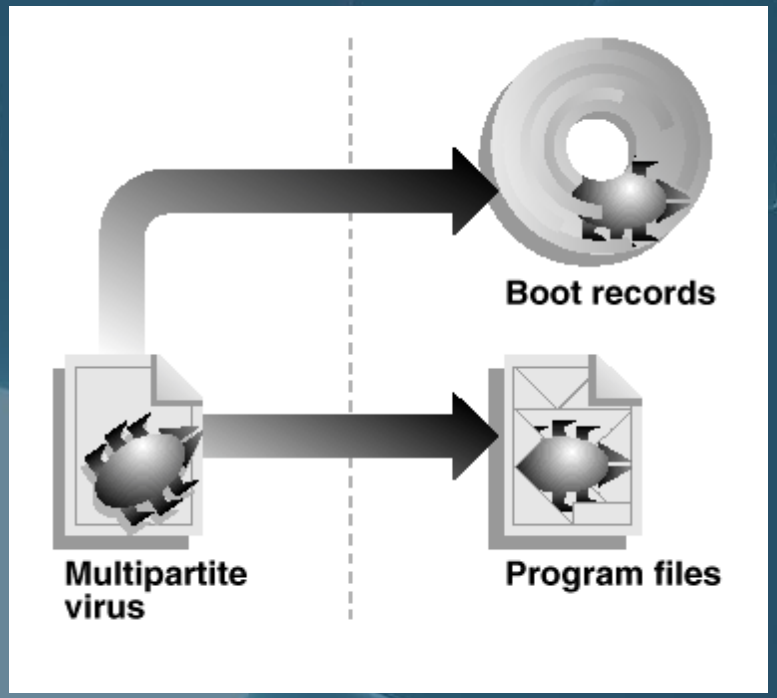
Vírustechnológiák



- Társvírusok
  - új fájlt hoz létre
  - az OS-t „utasítja”, hogy a kiválasztott fájl helyett az új hajtódjék végre (pl.: .EXE fájllal azonos .COM fájlt hoz létre, az OS a .COM-ot futtatja előbb)

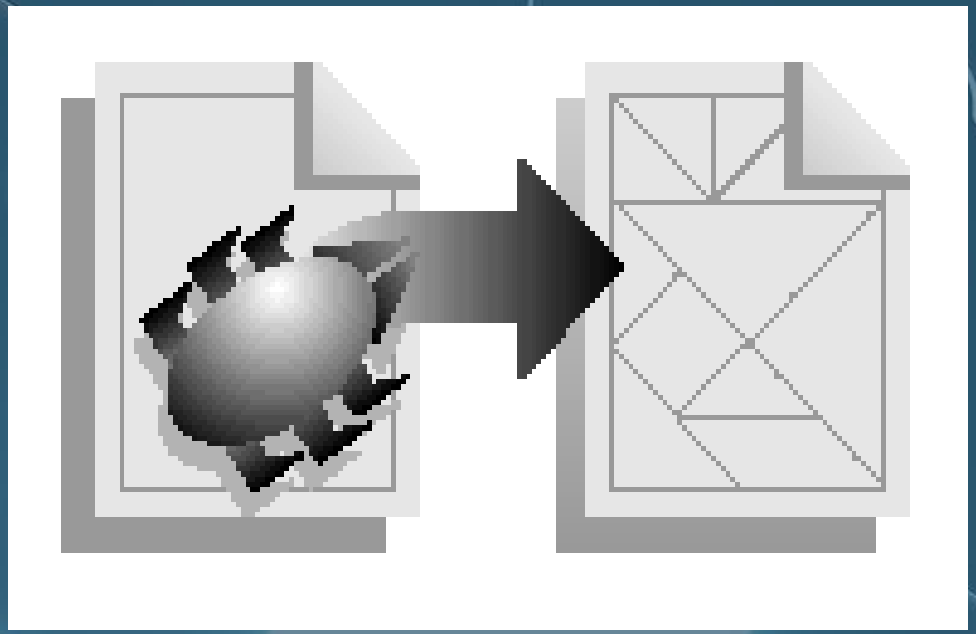
Vírustechnológiák

- Több módon fertőző vírusok
  - egyszerre program- és indítóvírusok (pl.: Tequila
    ⇩
    szövegszerkesztés
    ⇩
    indítórekord)



Vírusfertőzési ciklus 1.

Fertőzés



Fertőzés forrása lehet…

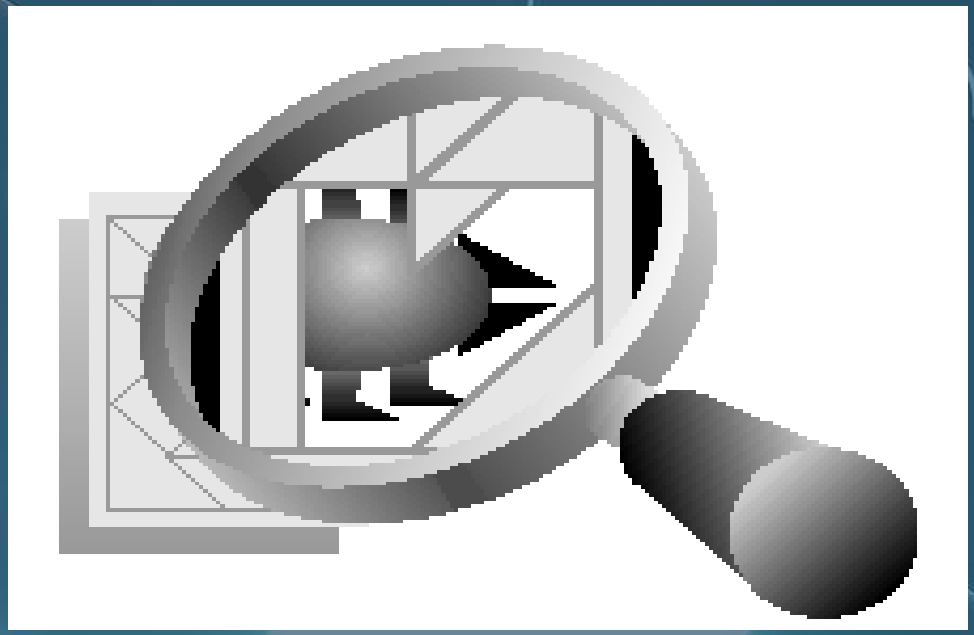
- Ismeretlen eredetű floppy használata
- Otthoni vagy iskolai lemez
- Barátoktól kölcsönkért lemez
- Nem megbízható kereskedőtől származó szoftver

Fertőzés forrása lehet…

- Kalóz szoftver
- Tömörített vagy megnyitott szoftver
- Internet szolgáltatótól letöltött program
- E-mail mellékletek

Vírusfertőzési ciklus 2.

Észlelés



Észlelés - megfigyelés

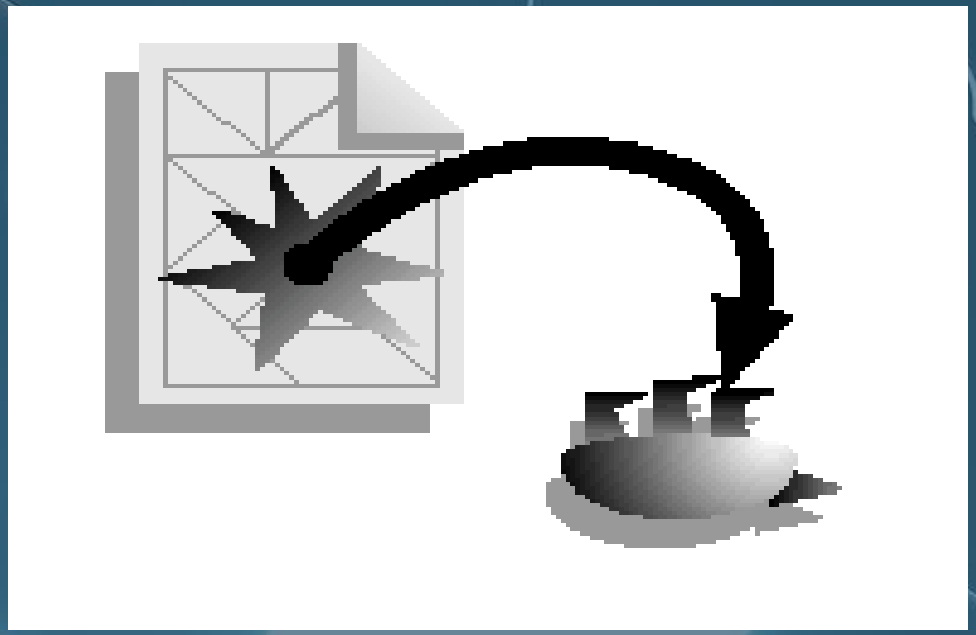
- Furcsa rendszerviselkedés
- Hiányzó fájlok
- Programok működésképtelensége

Észlelés

- Segédprogrammal
  - Víruselhárító szoftverrel észlelt vírus

Vírusfertőzési ciklus 3.

Helyreállítás



Helyreállítás - „Takarítás”

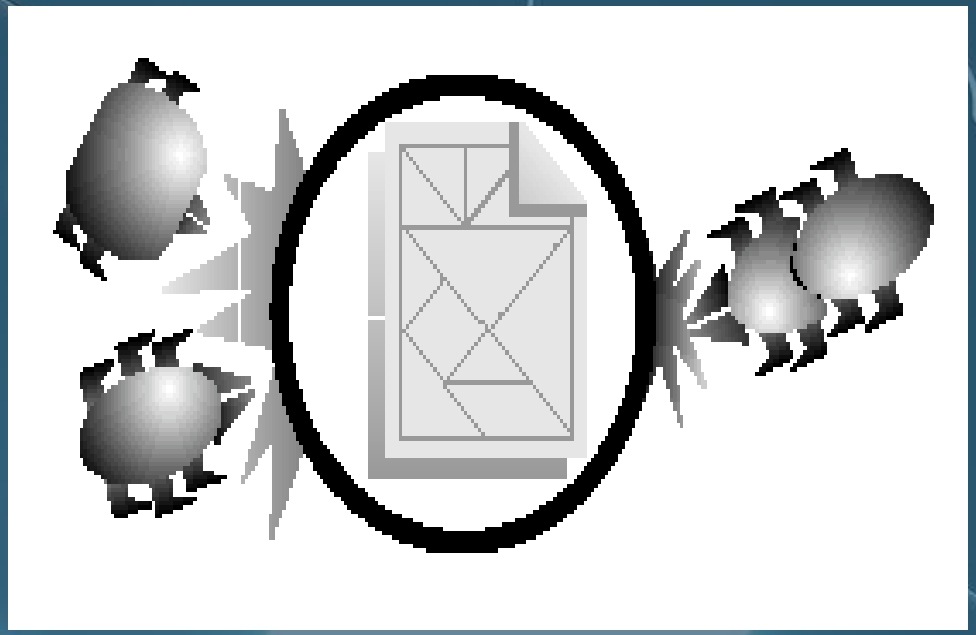
- Programok újratelepítése a mesterlemezről
- Fájlok kijavítása víruselhárító szoftverrel
- Visszaállítás fertőzésmentes biztonsági másolatról

Helyreállítást követően ...

- Az összes fájl újbóli vizsgálata a fertőzés forrásának megkereséséhez
- Az összes floppy újbóli vizsgálata a fertőzés forrásának megkereséséhez
- Az esetlegesen fertőzött biztonsági másolatok selejtezése
- Fokozott víruselhárítás egy ideig

Vírusfertőzési ciklus 4.

Megelőzés



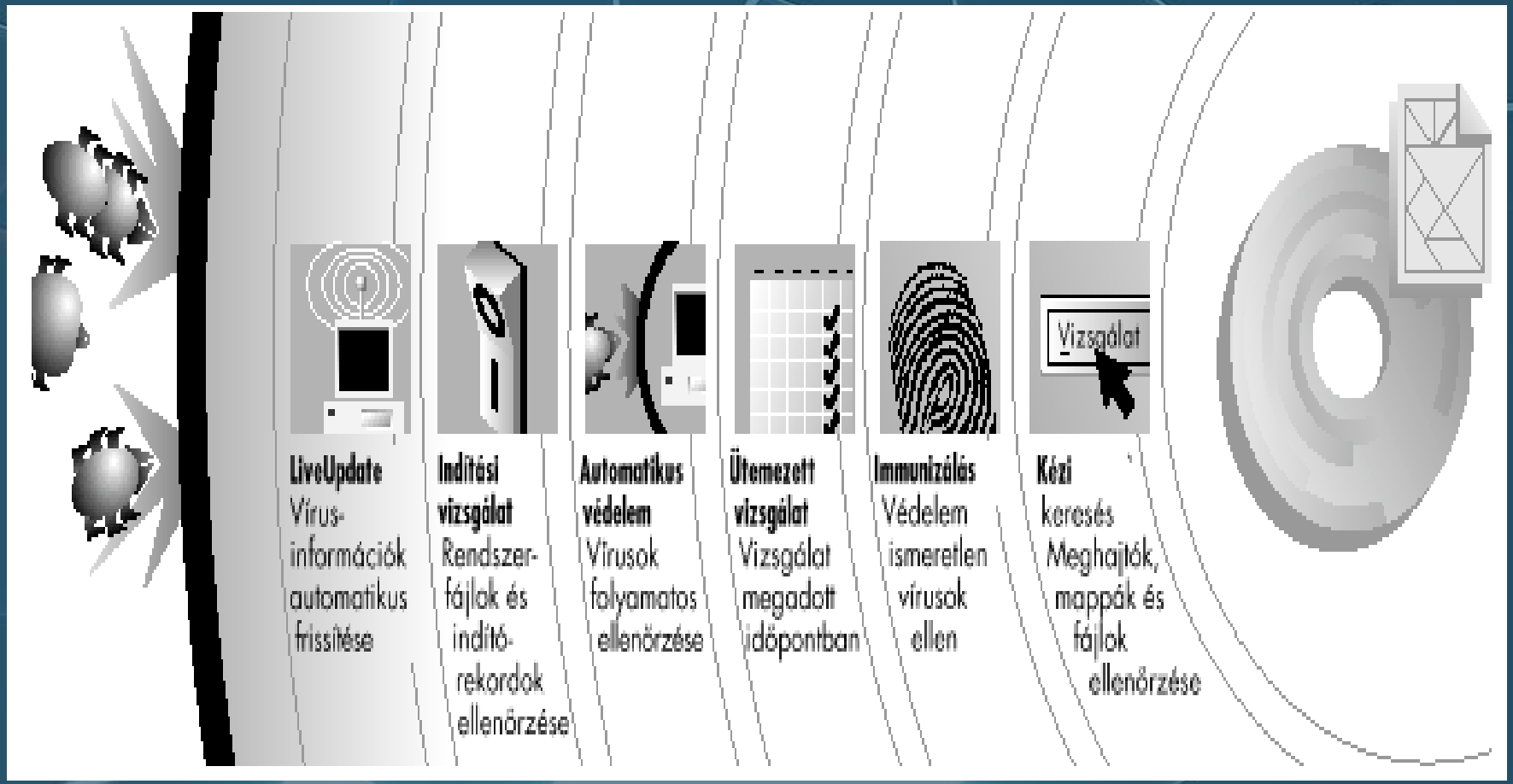
Megelőzés

- Vírusfigyelő programokkal:
  - Norton AntiVirus
  - NOD32
  - F-Secure (volt F-Prot)
  - VirusScan
  - VirusBuster ...

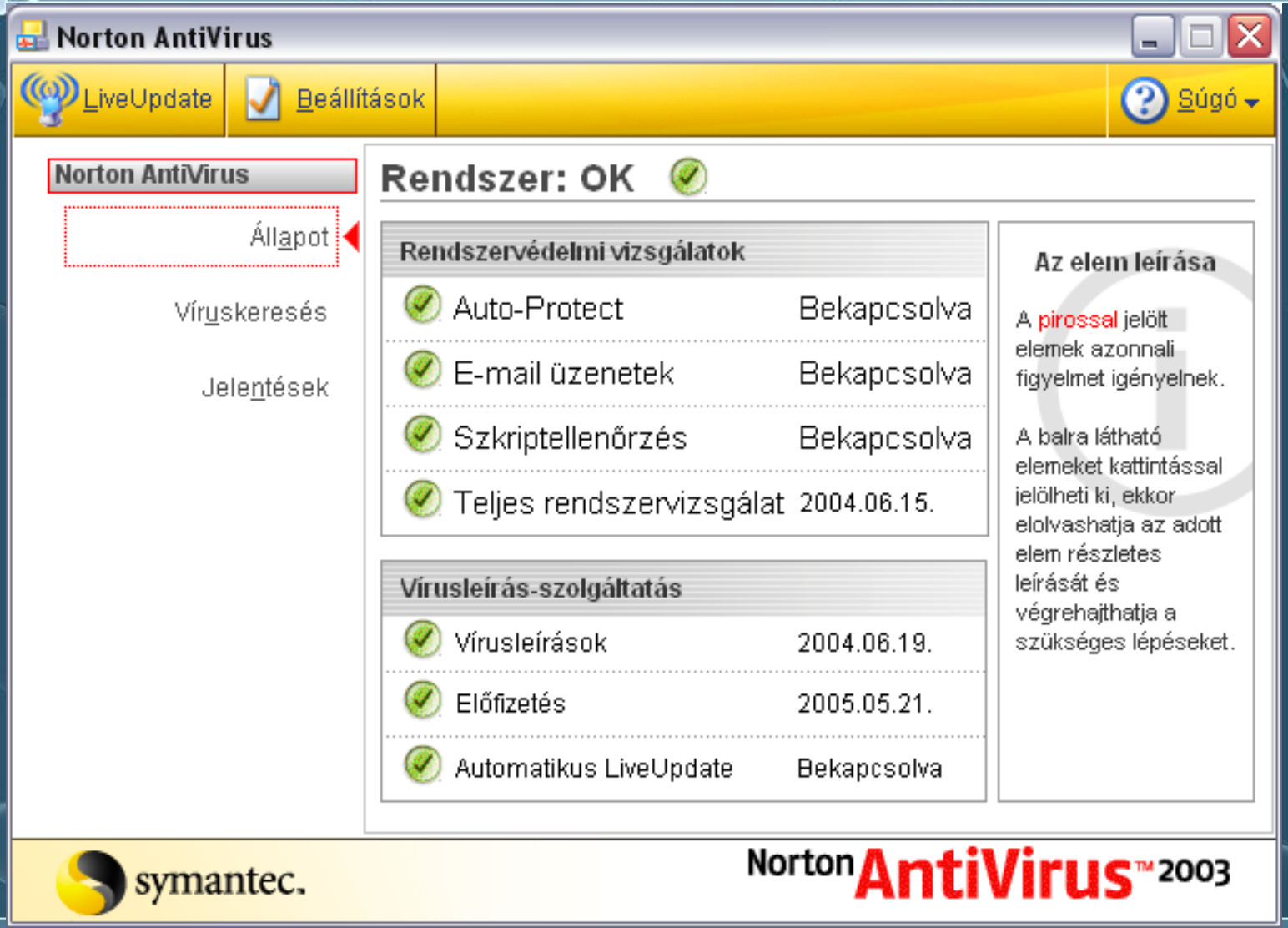
Alkalmazott keresési módok

- Aláírásos keresés
  - Már ismert vírusok kódjaival (aláírásával) dolgozik
  - 100%-os biztonságot nyújt
- Heuresztikus keresés
  - Valószínűsíti a vírustevékenységet
  - Kb. 80%-os biztonsággal ismeri fel

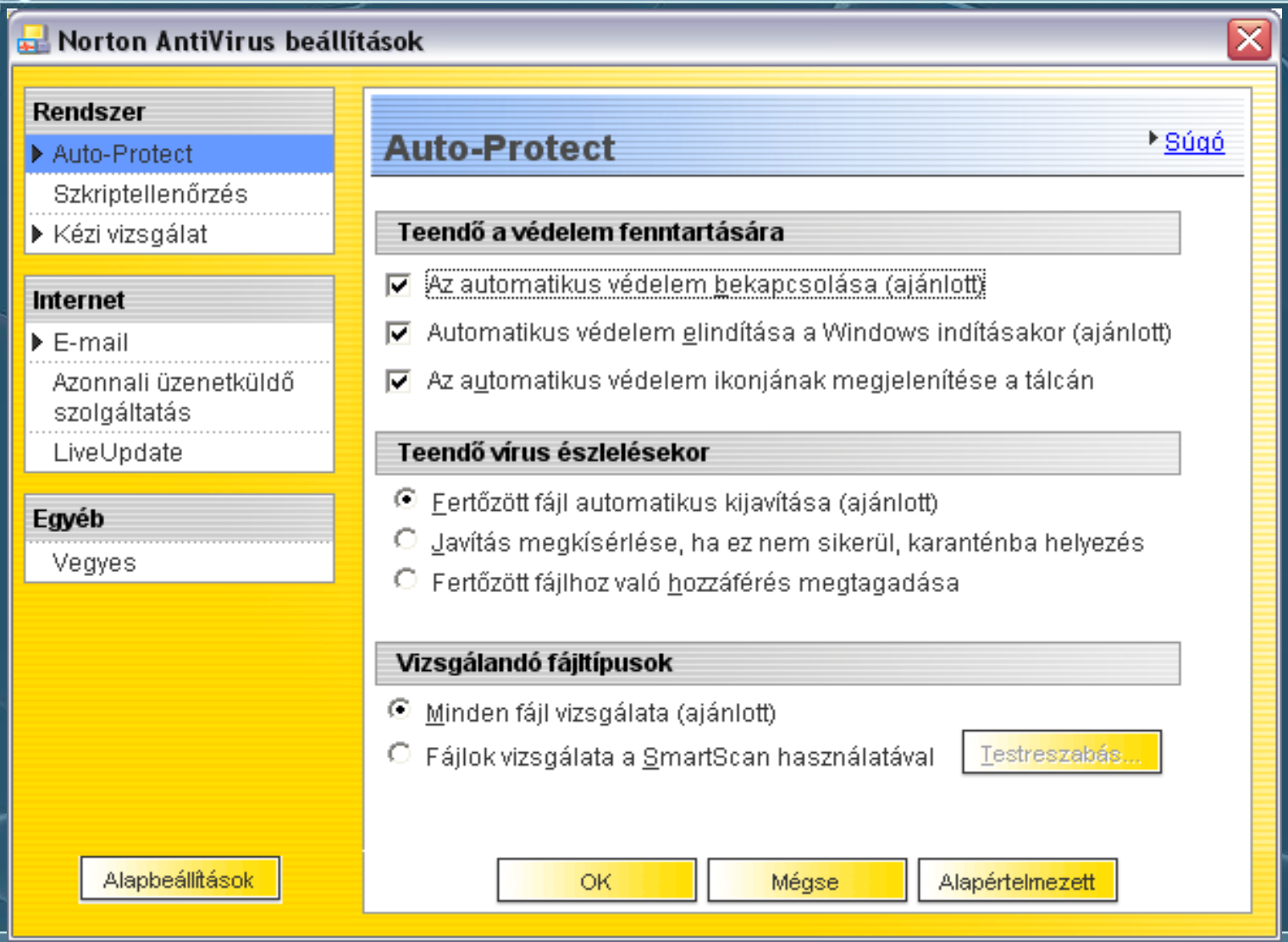
Norton AntiVirus védelme



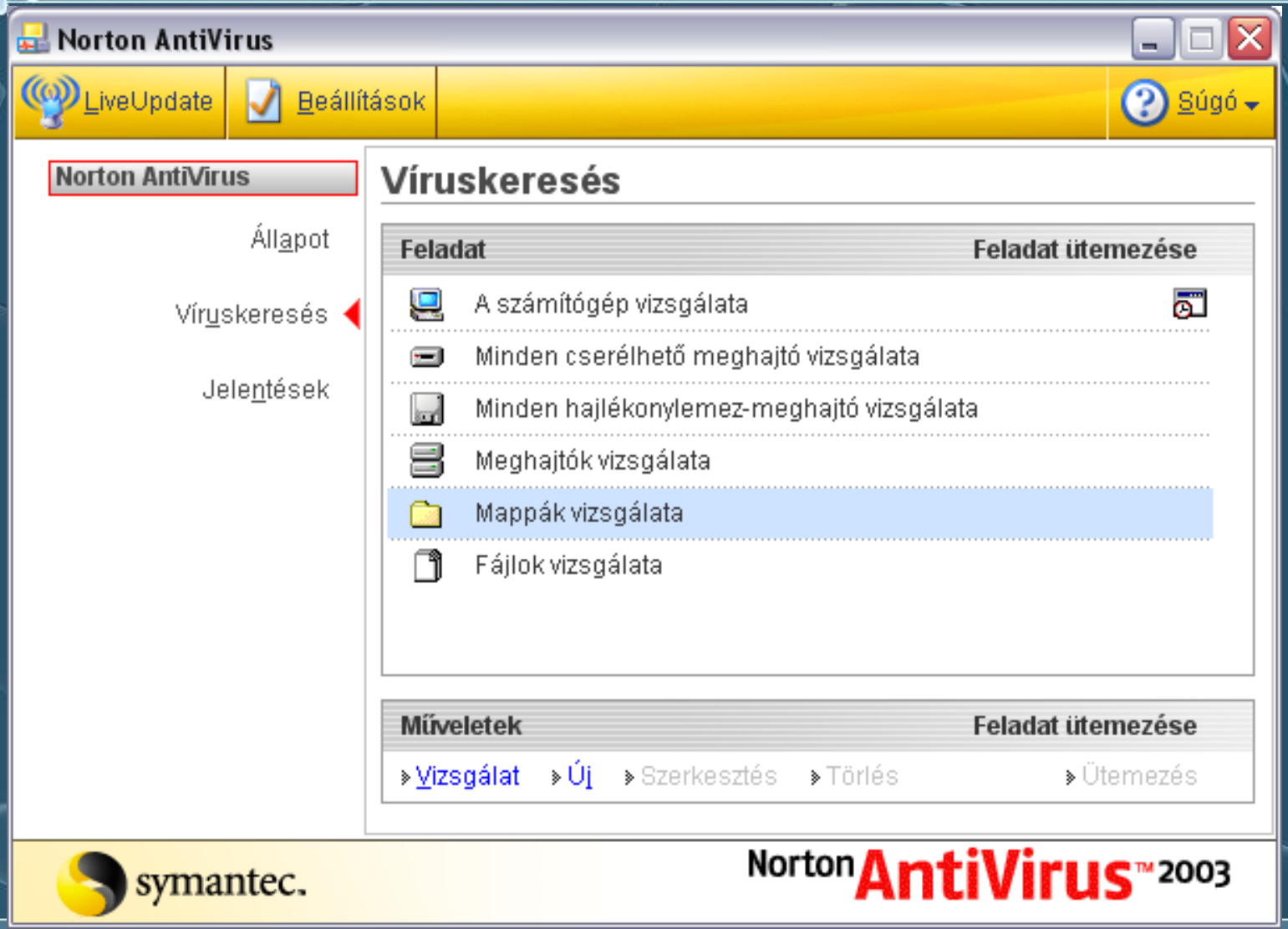
Norton AntiVirus védelme



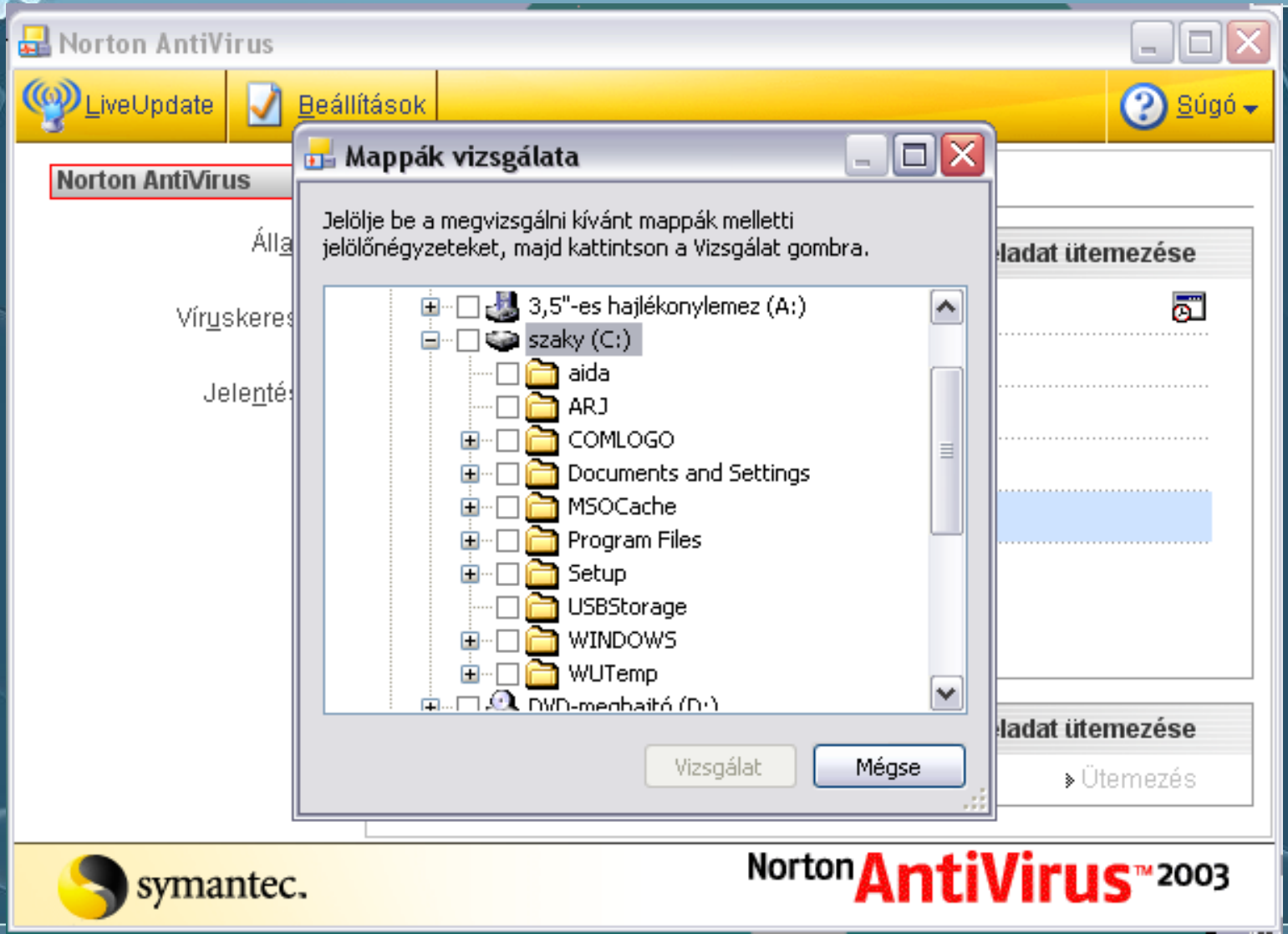
Norton AntiVirus védelme



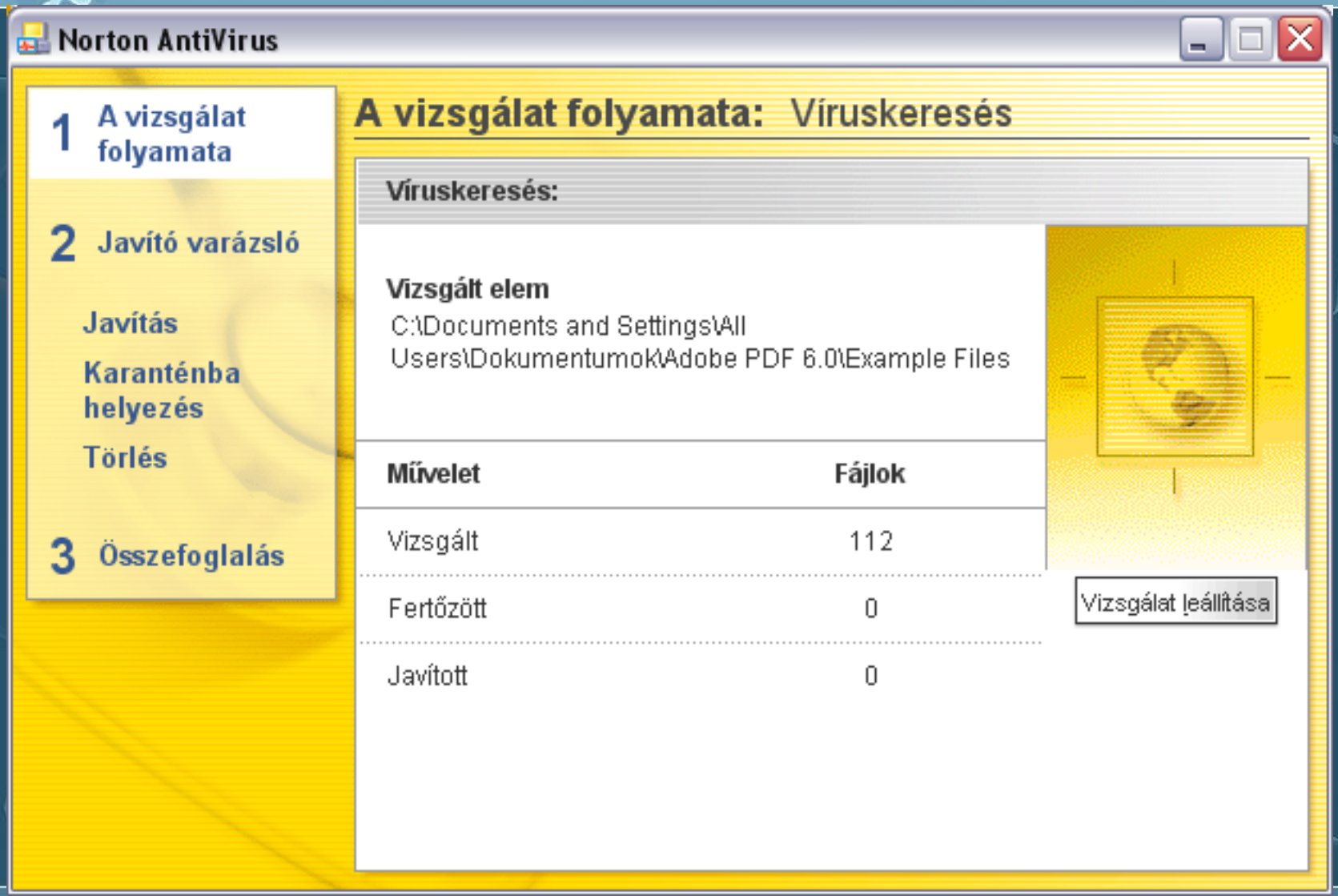
Norton AntiVirus védelme



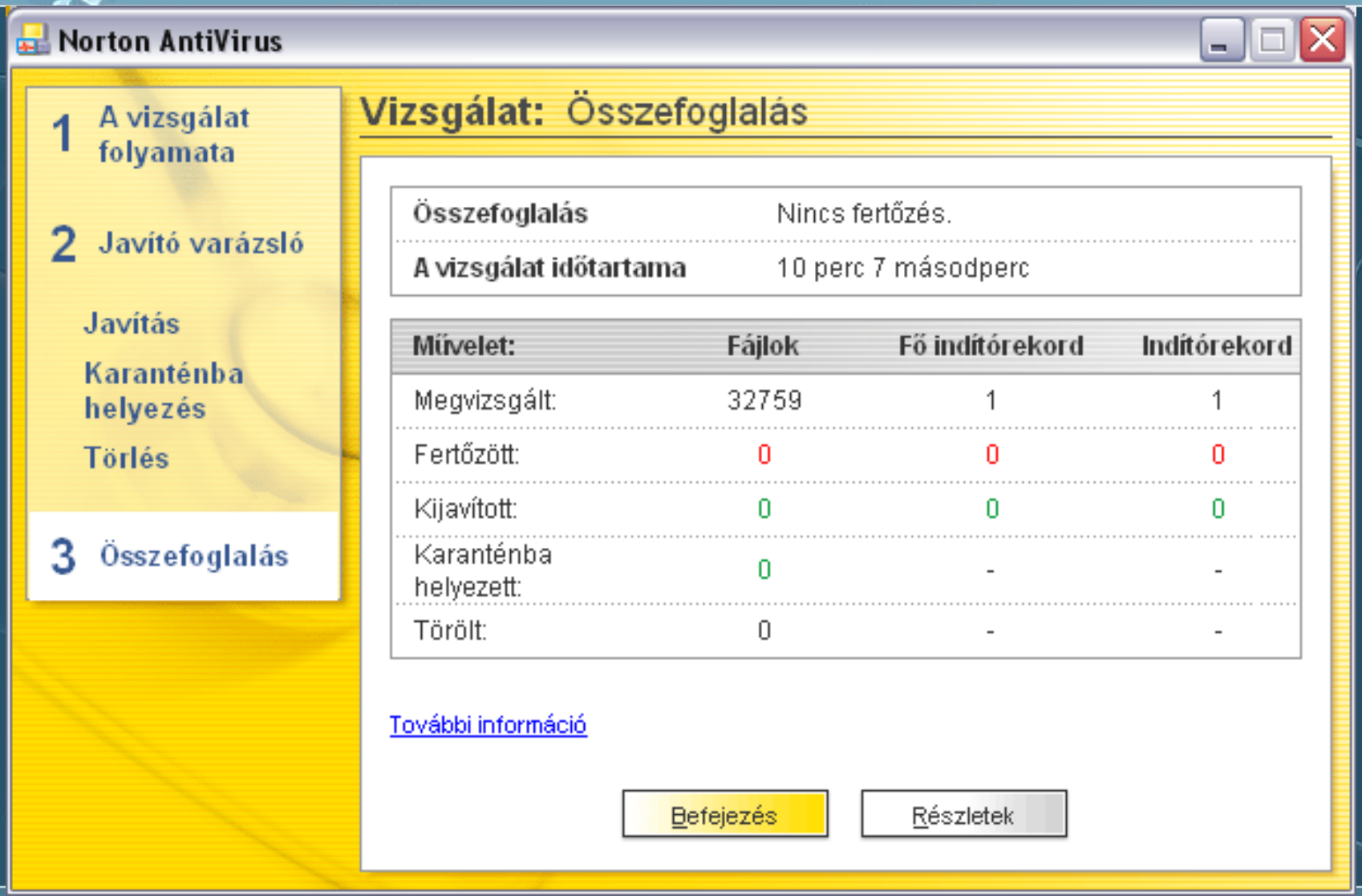
Norton AntiVirus védelme



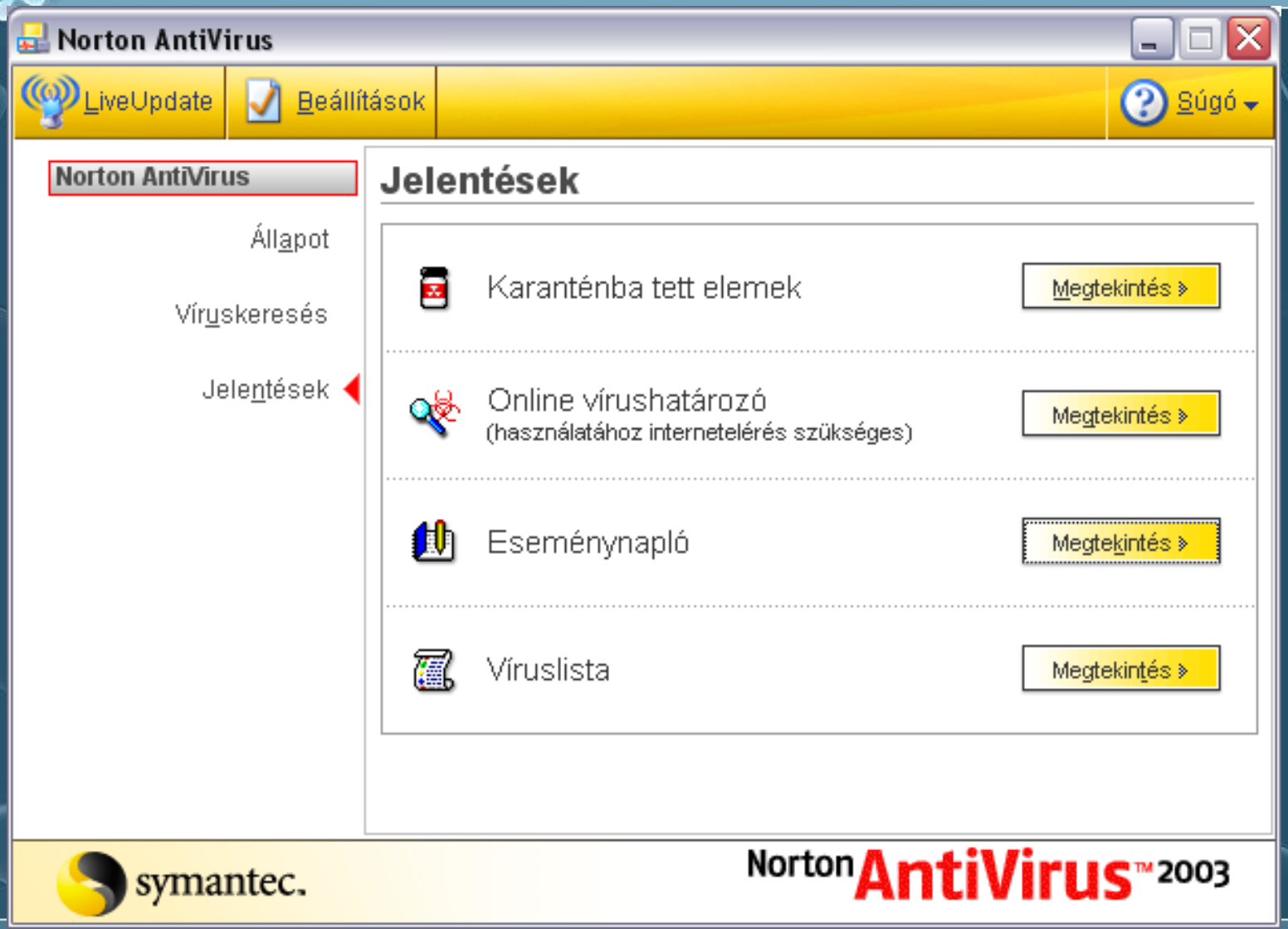
Norton AntiVirus védelme



Norton AntiVirus védelme



Norton AntiVirus védelme



Norton AntiVirus védelme