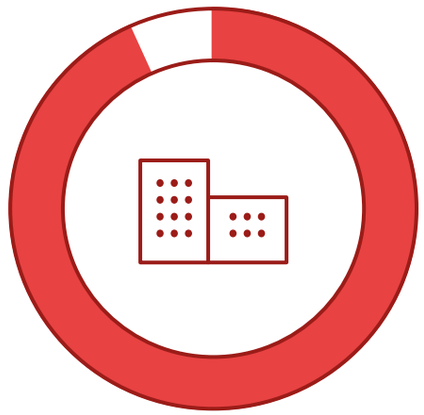
pandasecurity.com

Gyakorlati útmutató

a kiber zsarolások megelőzésére

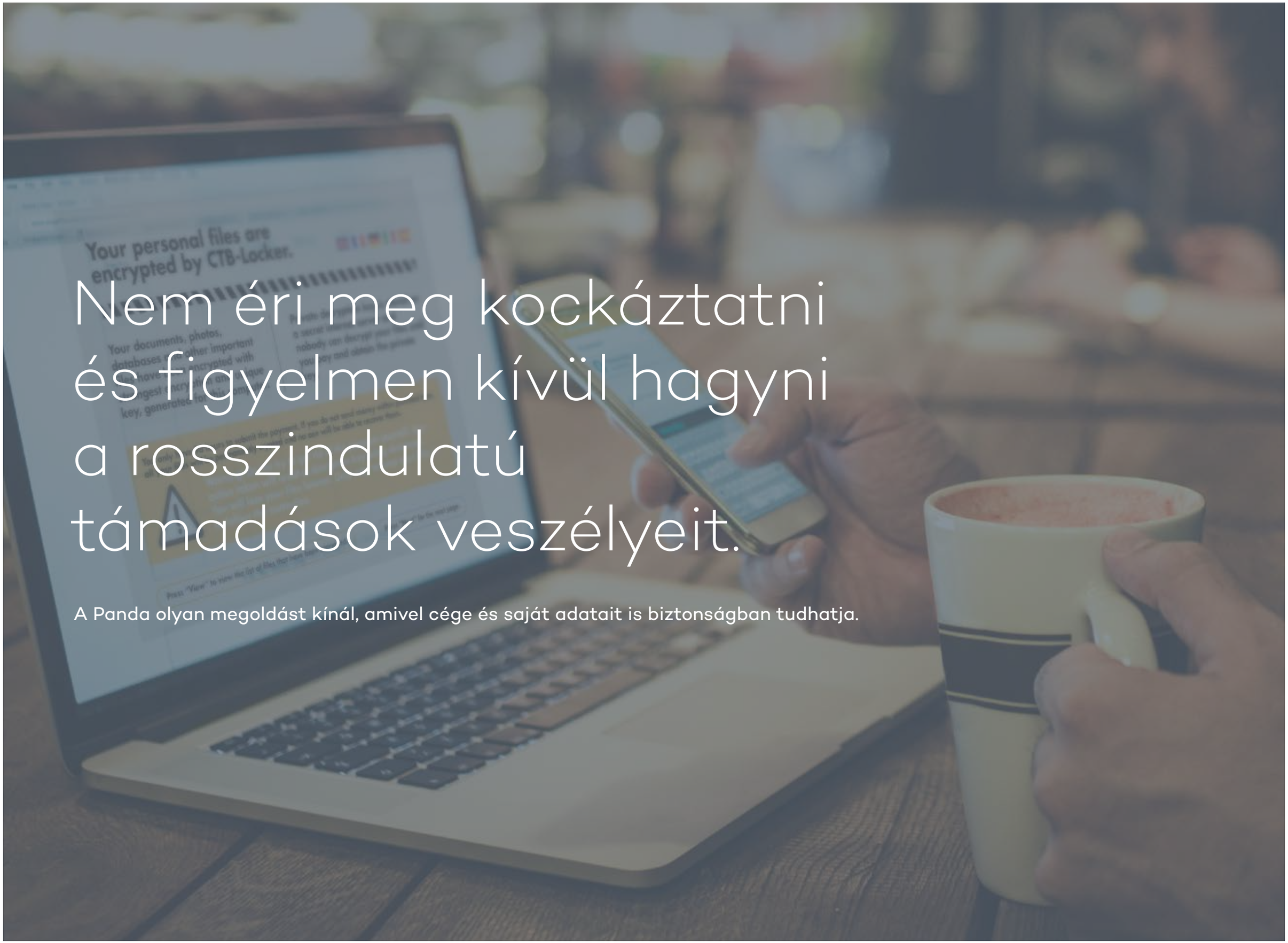
Az európai szervezetek
a károsultjai a legtöbb bizalmas
adatot érintő lopásnak.

Az előrejelzések azt mutatják, hogy 2016-ban tovább
folytatódnak az ilyen típusú számítógépes támadások.



A KKV-k 91%-a volt már
IT támadás áldozata

Forrás: Shopper Software Security in SMBs. Nielsen, April 2015



Nem éri meg kockáztatni és figyelmen kívül hagyni a rosszindulatú támadások veszélyeit.

A Panda olyan megoldást kínál, amivel cége és saját adatait is biztonságban tudhatja.

Mi az a kiber zsarolás?

A kiber zsarolás a fenyegetések egy olyan formája, mely esetén az informatikai támadás áldozatait a károk elkerülése érdekében, váltságdíj fizetésre kényszerítik.

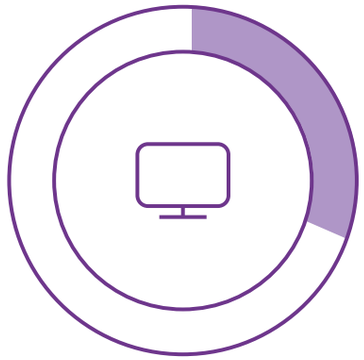
Az egyik legelterjedtebb módszer a számítógépes zsarolóprogramok használata. Az ilyen típusú kártevők titkosítják az áldozat számítógépén tárolt információkat, majd váltságdíjat követelnek az adatok visszaállításáért.

A váltságdíj kifizetését követően az áldozat rendszerint kap egy e-mailt az adatok visszaállításához szükséges kóddal. A fizetés rendszerint Bitcoinnal, egy valódi pénzre váltható virtuális fizető-eszközzel történik (1 Bitcoin = $ 380). Valójában, azért használják ezt a módszert, hogy a tranzakciót ne lehessen nyomon követni.

Sajnos azonban a váltságdíj kifizetése nem garantálja, hogy a cég a későbbiekben nem válik ismét hasonló zsarolás áldozatává.

Más hasonló kártevők, melyek megfertőzik a számítógépet, hozzáférhetnek a webkamerához és az azon keresztül rögzített tartalmak megosztásával zsarolják az áldozatot.

A legtöbb támadás e-mailben csatolt mellékletként, vagy rosszindulatú weboldalra mutató link formájában jut el a felhasználókhoz.



39%

Nem biztonságos, vagy csaló weboldal

23%

Szoftver letöltés

19%

e-mailben érkező fenyegetések

A fertőzések forrásai
Forrás: Shopper Software Security in SMBs. Nielsen, April 2015

Hogyan használják a kiber bűnözők a ransomware-eket támadásra?

A zsarolóvírusok, mint például a Cryptolocker, a Cryptowall, vagy a Coinvault a számítógépen található, vagy az elérhető hálózati meghajtókon található fájlok integritását veszélyeztetik.

A kártevő titkosítja az adatokat, melyeket csak akkor lehet visszaállítani, ha a cég kifizette a váltságdíjat a kiber bűnözőnek a visszaállításhoz szükséges kulcsért.

Amennyiben Ön áldozatává válik egy zsarolóvírusnak, rendszerint 48 vagy 72 óra áll rendelkezésre arra, hogy fizessen.

Amennyiben a megszabott idő alatt nem fizeti ki a váltságdíjat, későbbiekben annak akár többszörösét is követelhetik.

Ha a haladék lejárta után mégsem érkezik meg a pénz, a zsaroló törölheti a kulcsfájlt, ezzel lehetetlenné téve az adatok visszaállítását.

Még ha kifizetik a váltságdíjat, akkor sincs teljes garancia az adatok visszaszerzésére. Lehetséges, hogy a zsaroló által megalkotott szoftver olyan hibát tartalmaz, ami a dekódolás során adatvesztést eredményez, vagy a hatóságok már kísérletet tettek a bűnöző szervezet felszámolására.

Mi a teendő, ha kiber zsarolás áldozatává válik?

Ne engedjen a zsarolásnak, az ugyanis nem garancia a megoldásra.

Tény, hogy sok esetben, még ha fizet is az áldozat, nem kapja meg a kulcsot, vagy hibás kódot kap. Egyik esetben sem kapja vissza ellopott adatait.

Gyakori az ismételt zsarolás! Az adatok visszaszolgáltatása után a kiber bűnözők újabb titkosító alkalmazást telepítenek a gépre, amik azonnal folytatják az adatok titkosítását.

Más esetekben a bűnözők megemelik a váltságdíj összegét a cég pénzügyi helyzetének ismeretében az áldozat kétségbeesését kihasználva.

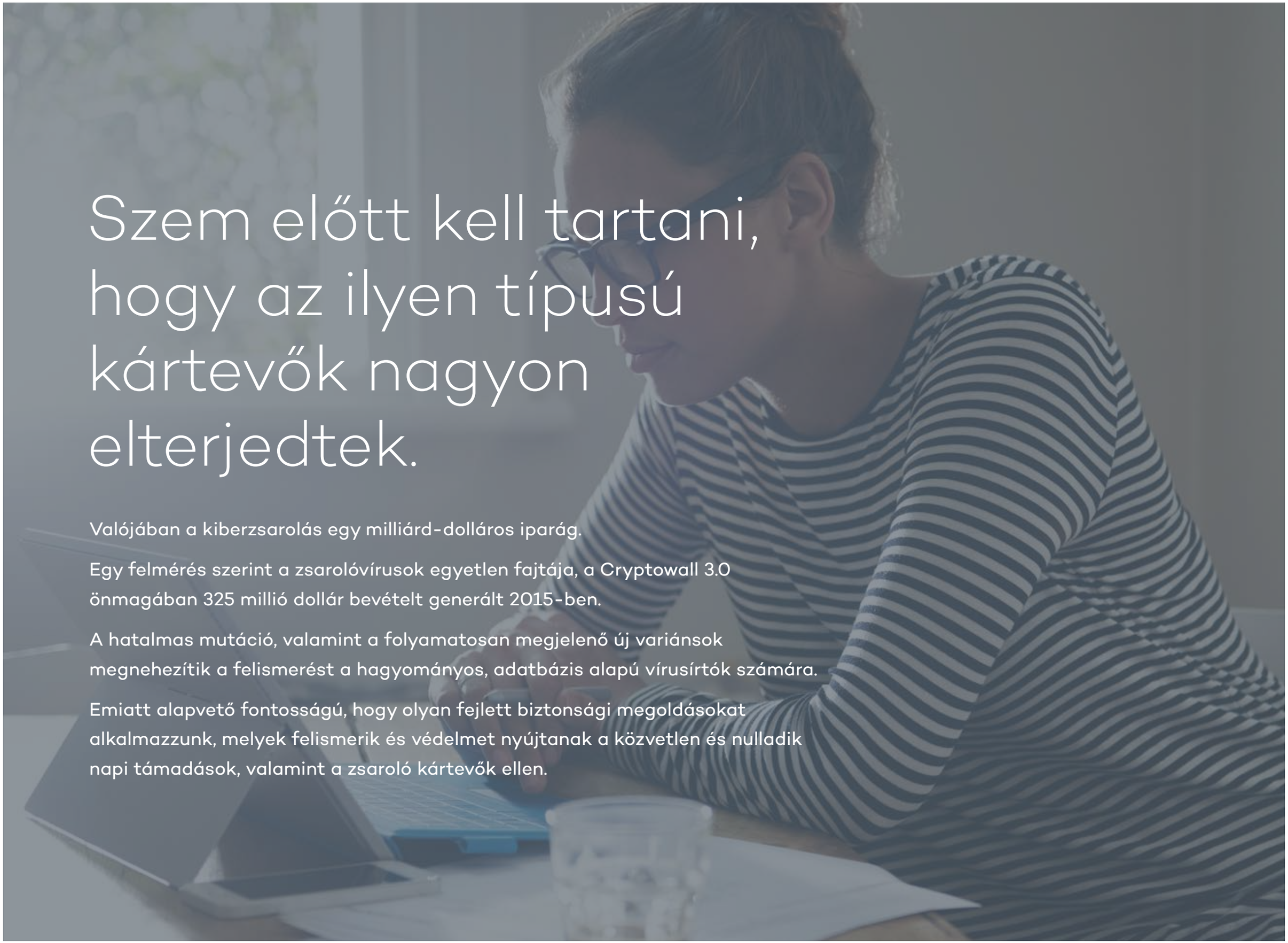
Távolítson el maradéktalanul minden kártevőt számítógépeiről.

Ehhez javasoljuk a Panda Cloud Cleaner offline módban történő használatát, mely eltávolít minden vírust a fertőzött számítógépekről.

Állítson helyre minden titkosított fájlt.

Ehhez szükséges, hogy előzőleg aktiválja a File Hystory-t (Windows 8.1 és 10 esetében) vagy a System Protection-t (Windows 7 és Vista esetében), mely lehetővé teszi a kártevő által módosított fájlok visszaállítását.

Javasoljuk továbbá, hogy minden fontos fájlról készítsen biztonsági mentést a lehető leggyakrabban. A helyreállítást megelőzően javasoljuk, hogy a mentett adatokat is vizsgálja át, hogy azok nem fertőzöttek-e.



Szem előtt kell tartani, hogy az ilyen típusú kártevők nagyon elterjedtek.

Valójában a kiberzsarolás egy milliárd-dolláros iparág.

Egy felmérés szerint a zsarolóvírusok egyetlen fajtája, a Cryptowall 3.0 önmagában 325 millió dollár bevételt generált 2015-ben.

A hatalmas mutáció, valamint a folyamatosan megjelenő új variánsok megnehezítik a felismerést a hagyományos, adatbázis alapú vírusírtók számára.

Emiatt alapvető fontosságú, hogy olyan fejlett biztonsági megoldásokat alkalmazzunk, melyek felismerik és védelmet nyújtanak a közvetlen és nulladik napi támadások, valamint a zsaroló kártevők ellen.

Mik a kártevők és melyek a leggyakoribb fajtái?

Nos, minden olyan program, vagy kód, melynek az a célja, hogy beszivárogjon a számítógépekre, vagy a hálózatokba és kárt okozzon, kémkedjen, vagy információkat tulajdonítson el.
A legveszélyesebb kártevő fajták:

RANSOMWARE (ZSAROLÓ VÍRUS)

Blokkolja a számítógép működését, megtiltja a felhasználói hozzáférést, titkosítja a fájlokat és váltságdíjat követel a visszaállításért.

EXPLOIT

Egy biztonsági hibát, vagy sebezhetőséget kihasználva a kommunikációs portokon keresztül hozzáférést biztosít a számítógéphez.

SPYWARE (KÉMPROGRAM)

Összegyűjti a neveket, hozzáférési adatokat, jelszavakat és bármilyen személyes, vagy céges információt.

PHISING (ADATHALÁSZAT)

Hamis URL-t hoz létre, hogy adatokat, személyes információkat, banki belépési adatokat lopjon el.

TROJAN (TRÓJAI)

Különböző alkalmazásokat telepít, amelyeken keresztül a hekkerek átveszik a számítógép felett az irányítást. Hozzáférnek a fájlokhoz és ellopják a bizalmas információkat.

APT (ADVANCED PERSISTENT THREAT- FEJLETT FOLYAMATOS FENYEGETÉS)

Ez egy olyan számítógépes folyamat, mely átjutva a biztonsági rendszereken ellenőrzi és figyeli a gépet és üzleti, vagy politikai céllal szivárogtat adatokat.

SCAM (ÁTVERÉS)

Különböző trükköket alkalmazva értesítéseket küld hamis akciókról, különféle nyereményekről, mint utazás, lottó nyeremény, azután a „díj” átvételéhez pénzt kér.

BACKDOOR (HÁTSÓAJTÓ)

Hátsóajtókat nyit a rendszer használatának átvételéhez.

KEYLOGGER (BILLENTYŰZET FIGYELŐ)

Összegyűjti és elküldi a felhasználó által leütött karaktereket.

BOT

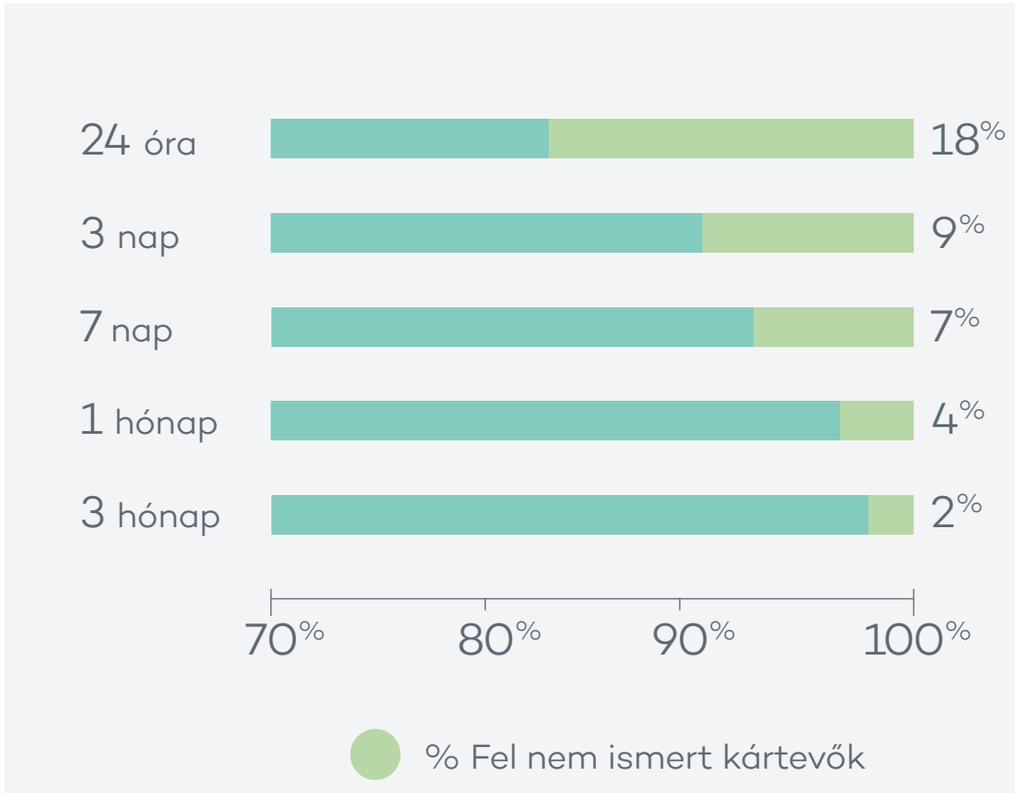
Egy program, melynek segítségével a számítógép távolról kezelhető.

WORM (FÉREG)

Megfertőzi a teljes számítógépet, lelassítja a hálózati forgalmat és blokkol minden kommunikációs csatornát.

A kártevők fejlődése, bonyolultsága és összetettsége.

A hagyományos vírusirtók által használt technológiák (adatbázis fájl, heurisztika) reaktívak. Az újonnan megjelenő kártevők 18%-a a hagyományos vírusirtók előtt rejtve marad az első 24 órában és 2% még 3 hónap múlva is ismeretlen.



Meg tudják állítani ezek az antivírusok a komolyabb fenyegetéseket?

Nem, az antivírus nem képes erre. Sőt, vannak olyan weboldalak, ahol le tudja ellenőrizni, hogy egy adott antivírus felismer-e egy bizonyos kártevőt. A hekkerek a rosszindulatú kódok terjesztése előtt szintén leellenőrzik, hogy az antivírus programok felismerik-e azt.

A Panda Security 5 javaslata a kiber támadások megelőzésére

1. Figyelmeztesse a felhasználókat

Ügyeljen rá, hogy a felhasználók legyenek tisztában az adathalászat veszélyeivel és ne töltsenek le ismeretlen, vagy a cég által nem jóváhagyott alkalmazásokat és ne nyissanak meg gyanús weboldalakat.

2. Legyen óvatos az interneten

Szabályozzák az internet használatot a káros oldalak elkerülése érdekében.

3. Használja az Önnek megfelelő megoldásokat

Győződjön meg róla, hogy olyan biztonsági megoldásokat használnak, melyek megfelelnek a cég igényeinek és folyamatosan tartsa azokat naprakészen.

Olyan megoldást, ami különböző biztonsági szintekkel rendelkezik, felismeri és blokkolja a komolyabb fenyegetéseket is.

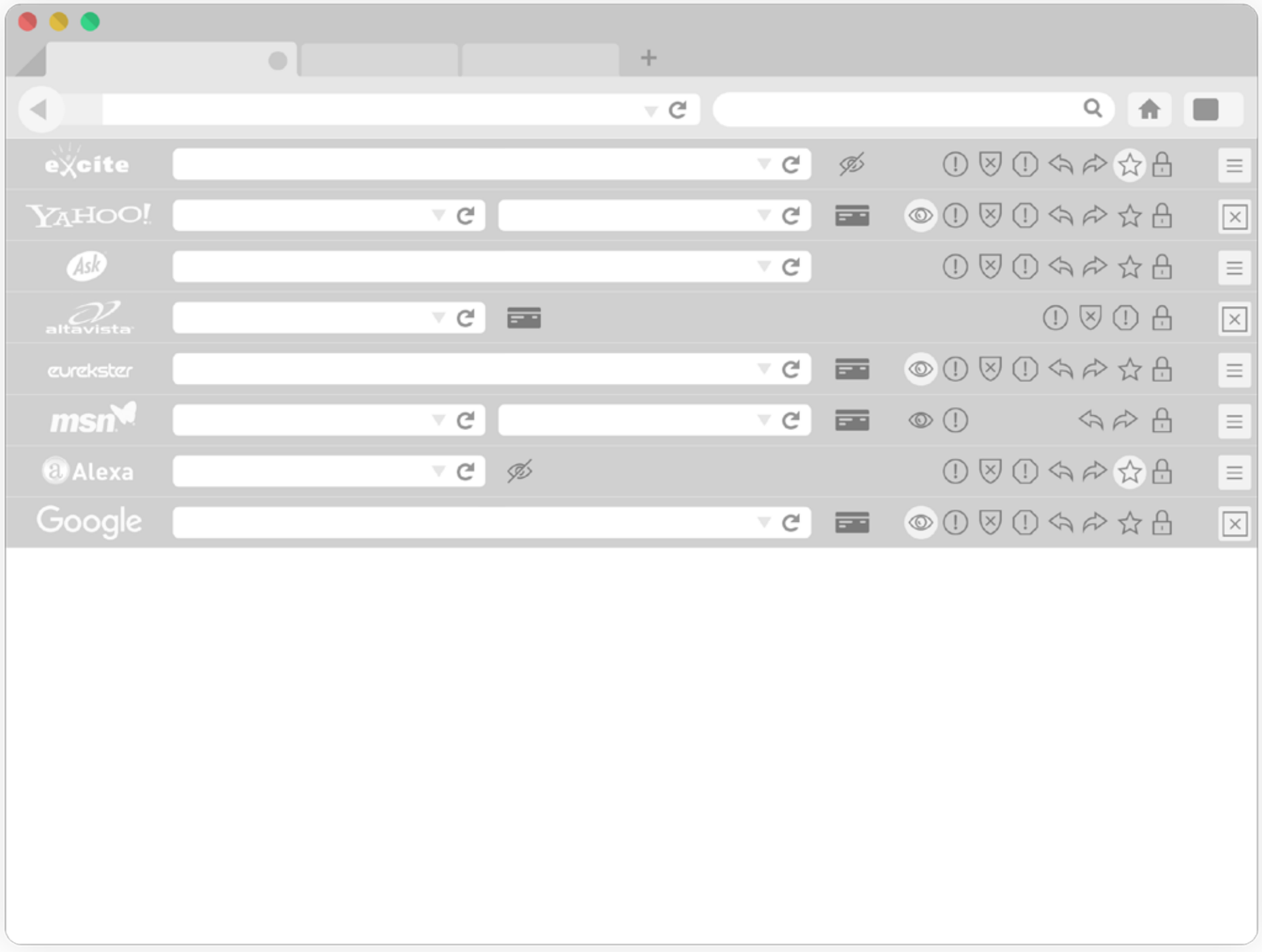
4. Alakítson ki belső protokollokat

Tegye meg a megfelelő biztonsági intézkedéseket a szoftverek telepítésének és futtatásának vizsgálatáért. Ellenőrizzék rendszeresen a telepített alkalmazások listáját.

5. Folyamatosan frissítse rendszerét és alkalmazásait

Határozza meg az alkalmazások frissítésére vonatkozó szabályokat, blokkolja, vagy kapcsolja ki azokat, amennyiben nem szükségesek.

Nagyon fontos, hogy védve legyenek a sebezhető alkalmazásoktól, még ha azok megbízható forrásból is származnak (mint pl. a Java, Office, Chrome, Mozilla vagy Adobe), mert ezek biztonsági réseit kihasználhatják a kiber bűnözők.



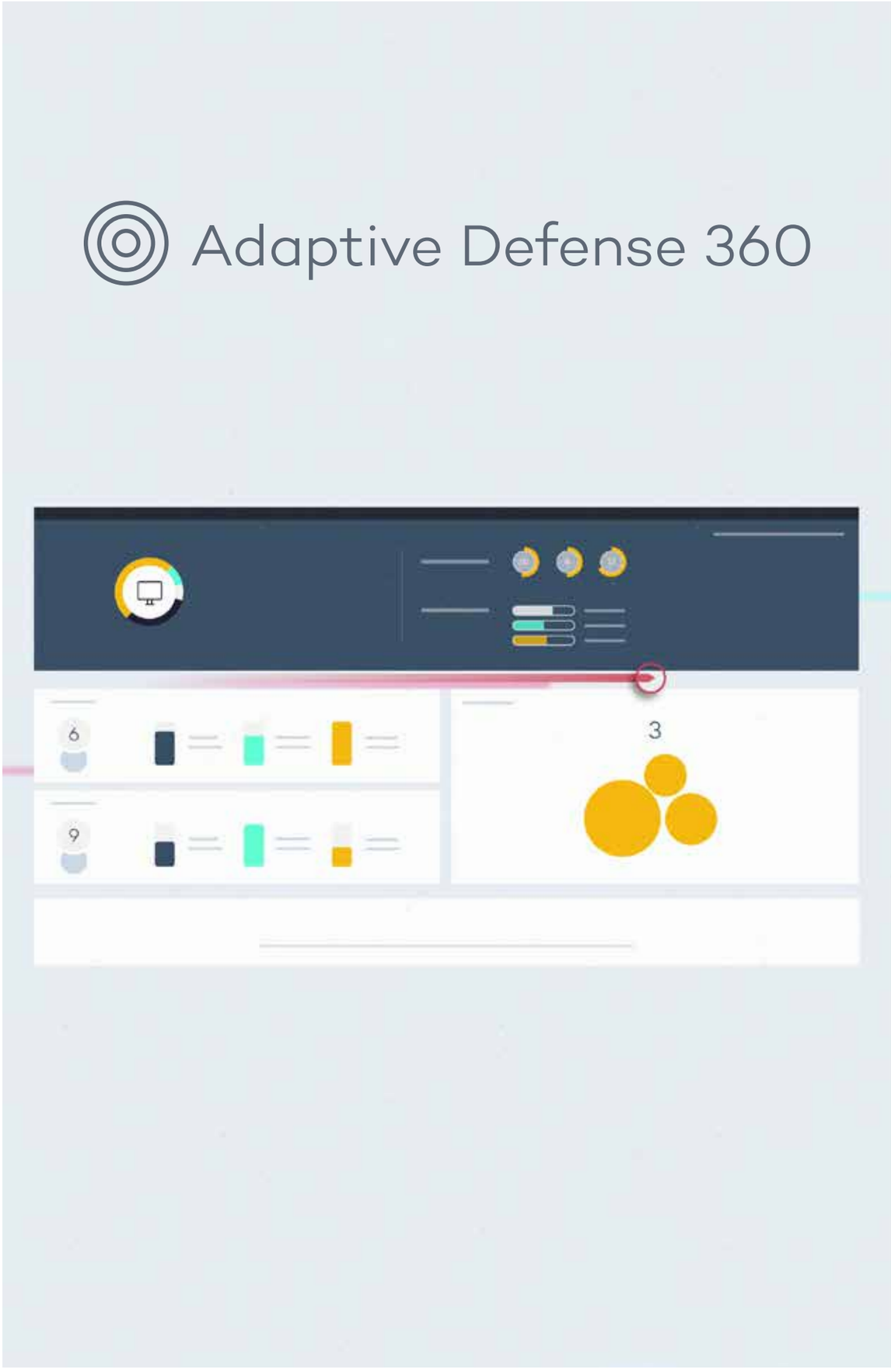
Kép: a böngésző eszköztárak nagy biztonsági kockázatot jelentenek

Hogyan tudja igazán megvédeni cégét?

A Panda Security kifejlesztette az első olyan megoldást, mely 100%-ban biztosítja az aktív folyamatok figyelését.

A Panda Security kifejlesztette az egyetlen olyan megoldást, mely képes megvédeni a vállalkozását a célzott támadásoktól, a nulladik napi kártevőktől, valamint a legújabb fenyegetésektől, beleértve a Cryptolockert is.

Ez az első olyan megoldás a piacon, mely teljes körű védelmet nyújt a számítógépek, szerverek részére a végpontokon futó folyamatok 100%-os ellenőrzésének köszönhetően.

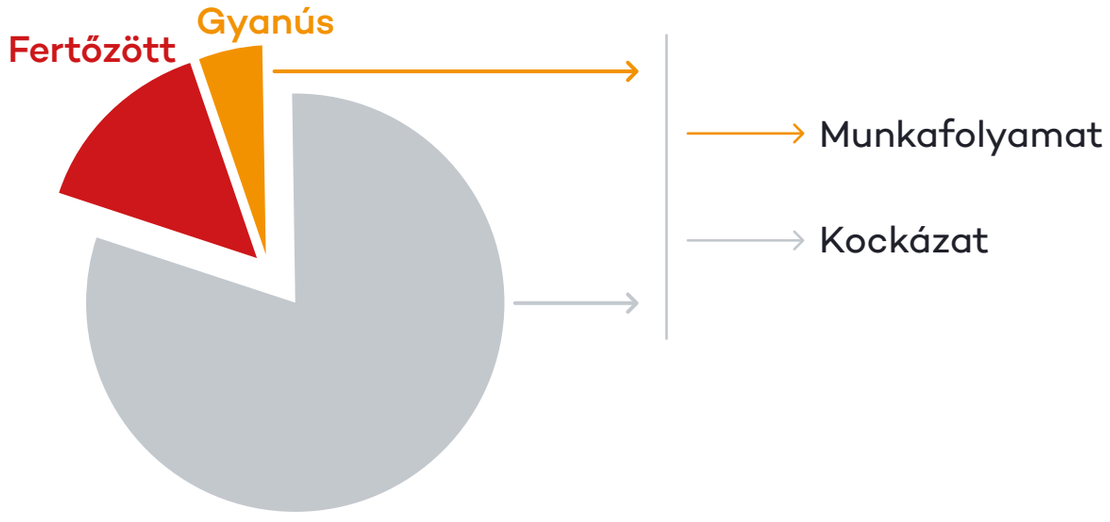


Az Adaptive Defense 360 a legmagasabb szintű biztonságot nyújtja, messze megelőzve a többi antivírus megoldást.

Az Adaptive Defense 360 figyeli, nyilván tartja és osztályozza a futó alkalmazások 100%-át, és az EDR funkciónak köszönhetően képes észlelni és blokkolni azokat a kártékony programokat is, amelyeket más rendszerek nem képesek felismerni.

Hagyományos antivírus

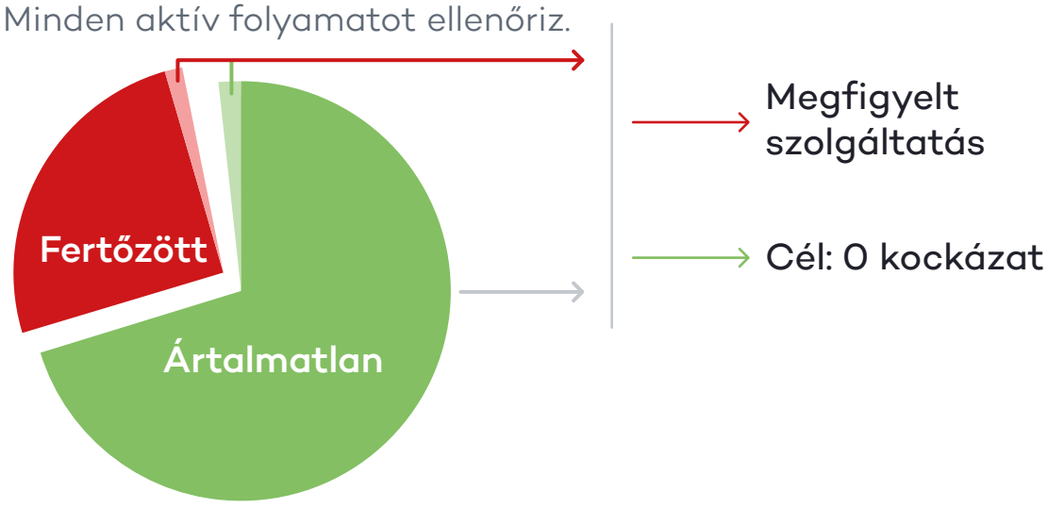
Csak a kártevőket ismeri fel, semmi mást.



Mivel nem képesek osztályozni a gyanús tevékenységeket, a támadások komoly biztonsági kihívást jelentenek a hagyományos antivírus programok számára (különösen a célzott támadások és a nulladik napi kártevők esetén).

Adaptive Defense 360

Minden aktív folyamatot ellenőriz.



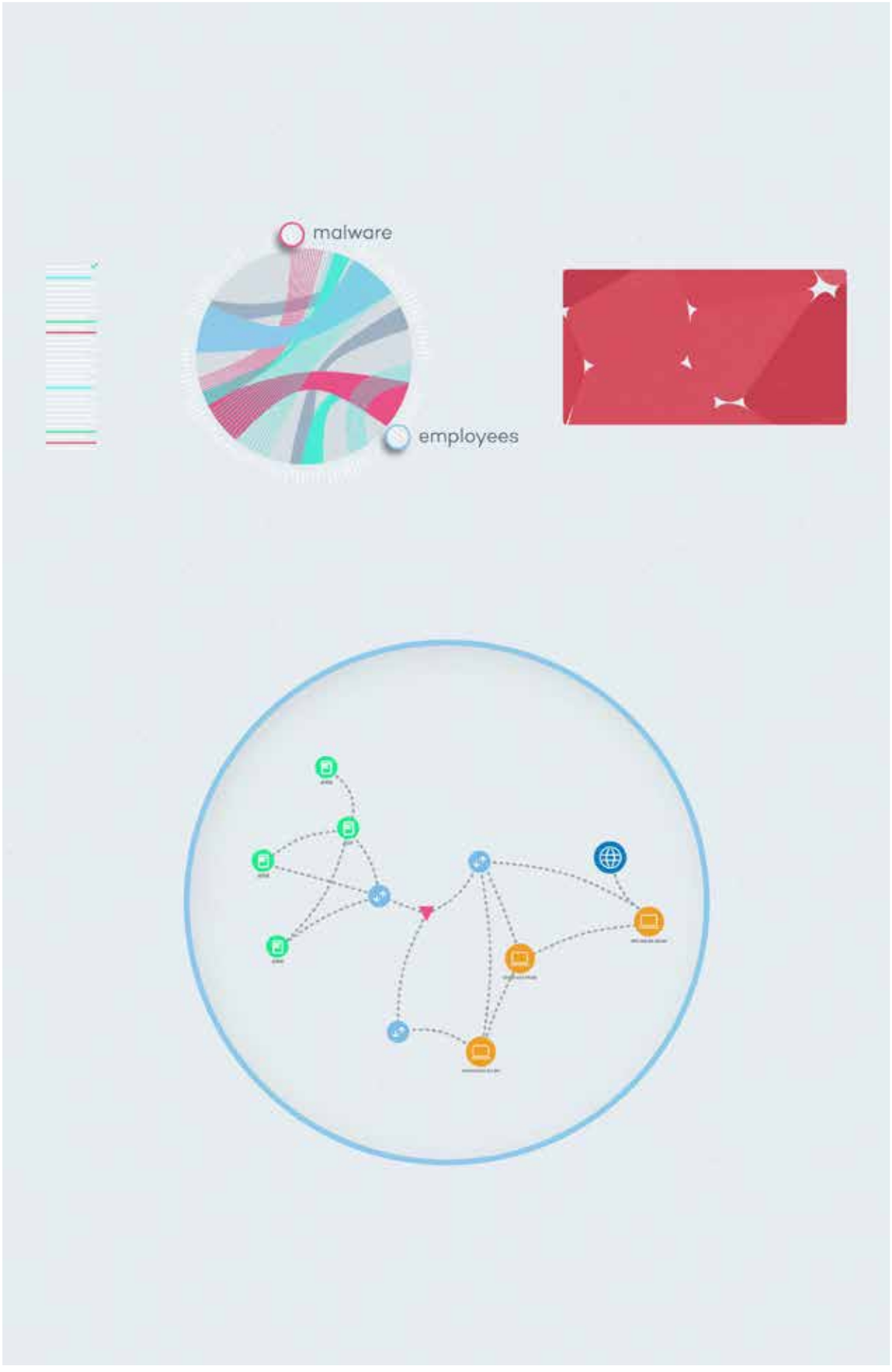
Az Adaptive Defense 360 biztosan tudja, ha egy folyamat ártalmatlan vagy káros. Kivétel nélkül osztályoz mindent, így a fenyegetés gyanúja sem merülhet fel.

Képes mindent ellenőrizni, ami a számítógépen történik, lehetővé téve ezzel, hogy:

Felismerje az adatszivárgást, legyen az külső vagy belső támadás, akár az archivált adatok esetén is (pdf, word, excel, txt...).

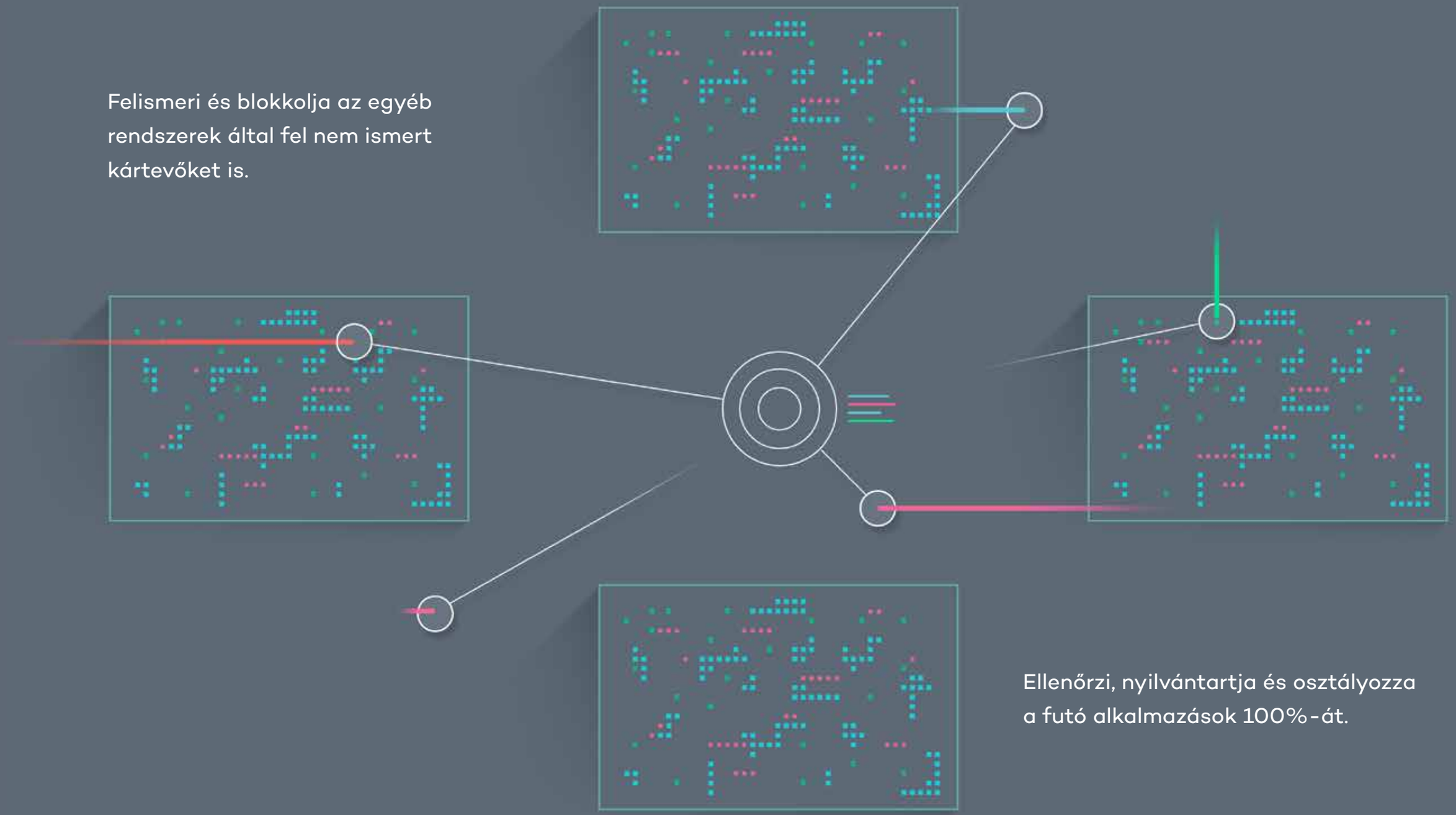
Felismeri és kijavítja a rendszerek és alkalmazások sebezhetőségeit, megakadályozva ezzel a nemkívánt alkalmazások használatát.

Érzékeli a rendszerét érintő célzott támadásokat.



Határtalan átláthatóság, teljes kontroll

Felismeri és blokkolja az egyéb rendszerek által fel nem ismert kártevőket is.



Ellenőrzi, nyilvántartja és osztályozza a futó alkalmazások 100%-át.

Az Adaptive Defense 360 számokban kifejezve

500K

Több mint 500 000 szervert és munkaállomást véd világszerte.

1.5M

Több mint 1.5 millió alkalmazást osztályozott

1.1M

Csak az elmúlt évben több mint 1 100 000 biztonsági sérülést enyhített.

550K

Több mint 550 000 óra IT erőforrást takarított meg, melynek becsült összege 34.8 millió Euro.

100%

100%-ban felismerte a kártevőket függetlenül a már telepített védelmi megoldásoktól.

2015-ös adatok

Mi több, a Panda Security 25 év szakmai tapasztalatával, és az innovatív megoldásoknak köszönhetően úttörőként szereppel a kártevők elleni küzdelemben.

Nem beszélve arról, hogy a Panda jelenleg több mint 30 millió végpontnak nyújt védelmet világszerte.

Contact us for more information

BENELUX
+32 15 45 12 80
belgium@pandasecurity.com

BRAZIL
+55 11 3054-1722
brazil@pandasecurity.com

FRANCE
+33 (0) 1 46842 000
commercial@fr.pandasecurity.com

GERMANY (AND AUSTRIA)
+49 (0) 2065 961-0
sales@de.pandasecurity.com

GREECE
+30 211 18 09 000
greece@pandasecurity.com

HUNGARY
+36 1 224 03 16
hungary@pandasecurity.com

ITALY
+39 02 24 20 22 08
italy@pandasecurity.com

MEXICO
+52 55 8000 2381
mexico@pandasecurity.com

NORWAY
+47 93 409 300
norway@pandasecurity.com

PORTUGAL
+351 210 414 400
geral@pt.pandasecurity.com

SPAIN
+34 900 90 70 80
comercialpanda@pandasecurity.com

SWEDEN (FINLAND & DENMARK)
+46 0850 553 200
sweden@pandasecurity.com

SWITZERLAND
+41 22 994 89 40
info@ch.pandasecurity.com

UNITED KINGDOM
+44 (0) 844 335 3791
sales@uk.pandasecurity.com

USA (AND CANADA)
+1 877 263 3881
sales@us.pandasecurity.com