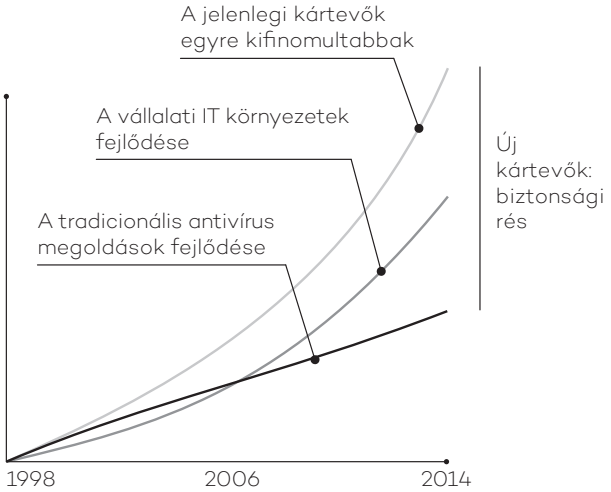
Adaptive Defense

Szüntesse meg a fejlett fenyegetések számára elérhető biztonsági réseket

www.kibertamadasok.hu
+36 1 224 0316
hungary@hu.pandasecurity.com

ÚGY GONDOLJA, HOGY AZ ÖN VÁLLALATA VÉDETT A NULLADIK NAPI, VALAMINT A CÉLZOTT TÁMADÁSOKKAL SZEMBEN?

A kártevők és az IT biztonság körképe jelentős változáson ment keresztül mennyiség és kifinomultság tekintetében is. Az aktív kártevők száma exponenciálisan megnövekedett (körülbelül 400.000 új vírus jelenik meg naponta), valamint a védelmek áttörésére és a kártevők elrejtésére irányuló új technológiák lehetővé teszik a fenyegetések számára, hogy a vállalati hálózaton hosszú ideig észrevehetetlenek maradjanak.



Mindeközben az informatikai környezetek fokozatosan összetettebbé váltak, ezáltal nehezebben menedzselhetővé és sebezhetőbbé téve a vállalati IT rendszereket.

A tradicionális antivírus megoldások már nem tudnak lépést tartani a valósággal. Lineáris fejlődésük továbbra is olyan idejétmúlt felismerési technikákon alapul, mint az adatbázis fájlok és a heurisztikus algoritmusok. Ennek következtében eredményeik pontatlanok lesznek, például a kártevők észrevétlenek maradnak, vagy téves riasztásokat generálnak.

Ez az összeférhetetlenség vezettet ahhoz, amit ma úgy hívnak **„biztonsági rés a kártevők számára”**: egy újonnan megjelent kártevő és a vírusvédelmi vállalatok által kiadott ellenszer megjelenése közötti időszak.

Egy egyre növekvő rés, melyet a hackerek kihasználnak, hogy vírusokat, ransomware-eket, trójaiakat és egyéb kártevőket juttassanak a vállalati hálózatokra.
Ezek az egyre gyakoribb fenyegetések titkosíthatják a bizalmas dokumentumokat és váltságdíjat követelhetnek értük, vagy egyszerűen összegyűjthetik a kényes adatokat, akár ipari kémkedés céljából.

A kormányok, bankok és egyéb nagyvállalatok mellett ma már a kis- és középvállalatok is elszenvedői azon támadásoknak, melyeket a tradicionális antivírusok nem képesek időben észlelni. Saját Kutatási Részlegünk vírusminták millióit és a legjobb antivírus termékeket elemezte, hogy igazolja: a kártevők 18%-a észrevétlen marad a kiadásukat követő 24 órában, sőt ezen hagyományos vírusvédelmi megoldások 3 hónap elteltével sem képesek észlelni az új kártevők 2%-át.

A megoldás erre a helyzetre az **Adaptive Defense**: a Panda Security szolgáltatása, mely képes pontosan osztályozni minden, a rendszerben futó alkalmazást, ezzel lehetővé téve, hogy csak a kívánt programok futhassanak.

Ennek eléréséért 5 éven át dolgoztunk egy **új biztonsági modell**en, mely három fő elven alapszik: a vállalat számítógépein és szerverein futó alkalmazások folyamatos megfigyelése; automatikus besorolás a felhőben lévő Big Data platformon alkalmazott gépi tanulás használatával; és végül a műszaki szakértőink elemzése – akik azon alkalmazásokat elemzik, melyek nem kerültek automatikusan besorolásra - annak érdekében, hogy megbizonyosodjanak minden, a vállalat rendszerein futó alkalmazás viselkedéséről.

Adaptive Defense

Szüntesse meg a fejlett fenyegetések számára elérhető biztonsági réseket

www.kibertamadasok.hu
+36 1 224 0316
hungary@hu.pandasecurity.com

AZ EGYETLEN MEGOLDÁS, AMI GARANTÁLJA AZ ÖSSZES FUTÓ ALKALMAZÁS BIZTONSÁGÁT

TELJES ÉS ROBOSZTUS GARANTÁLT VÉDELEM

A **Panda Adaptive Defense** kétféle üzemmódot kínál:

- A **normál üzemmód** engedélyezi az összes goodware-ként katalogizált alkalmazás futását azon alkalmazásokkal együtt, melyek még nem kerültek besorolásra a Panda Security, vagy az automatizált rendszerek által.
- A **kiterjesztett üzemmód** csak a goodware-ek futását engedélyezi. Ez az ideális védelmi forma azon vállalatoknak, akik a 'kockázatmentes' megközelítéssel állnak a biztonsághoz.

FORENSIC (NYOMELEMZŐ) INFORMÁCIÓK

- A **Végrehajtott Események grafikon** tiszta, átlátható képet ad a kártevők által okozott összes eseményről.
- A megoldás vizuálisan megjelenő információt nyújt a kártevők kapcsolatainak, létrehozott fájljainak és még sok más információnak a földrajzi forrásáról a **hőtérképek** segítségével.
- Lokalizálja a hálózatra telepített, közismert sebezhetőséggel rendelkező szoftvereket.

KOMPATIBILIS A TRADICIONÁLIS ANTIVÍRUS MEGOLDÁSOKKAL

Az **Adaptive Defense** a vállalat végpont eszközein egyidőben tud működni a tradicionális antivírus megoldásokkal és azokat a kártevőket is blokkolja - beleértve a célzott és a nulladik napi támadásokat, melyeket egy tradicionális megoldás nem lenne képes észlelni.

VÉDELEM A SEBEZHETŐ OPERÁCIÓS RENDSZEREK ÉS ALKALMAZÁSOK SZÁMÁRA

Az olyan rendszerek mint a Windows XP, melyek már nem támogatottak a gyártó által, ezáltal nem frissítettek és sebezhetőek, könnyű áldozatává válnak a nulladik napi és az újgenerációs támadásoknak. Továbbá, az olyan alkalmazások, mint a Java, Adobe, Microsoft Office és a böngészők sebezhetőségeit 90%-ban kihasználják a kártevők.
Az **Adaptive Defense** Sebezhetőség Védelmi Modulja tartalmi és viselkedési szabályokat használva biztosítja a vállalatok számára a biztonságos környezetben való munkavégzést, még akkor is, ha az általuk használt rendszerek nem naprakészek.

FOLYAMATOS INFORMÁCIÓ A HÁLÓZAT ÁLLAPOTÁRÓL

- A megoldás azonnali értesítéseket küld abban a pillanatban, ahogy a kártevő észlelésre kerül a hálózatban, egy átfogó jelentés segítségével, mely részletezi a kártevő helyzetét, a fertőzött számítógépeket és a kártevő által indított tevékenységeket.
- A szolgáltatás napi tevékenységéről e-mailben küld jelentéseket.

ELÉRHETŐ SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT- INFORMÁCIÓBIZTONSÁGI ÉS ESEMÉNYMENEDZSMENT)

Az **Adaptive Defense** összefonódik a SIEM megoldásokkal annak érdekében, hogy részletes adatokat nyújtson a rendszerekben futó összes alkalmazás tevékenységéről.

A SIEM nélküli ügyfelek számára az **Adaptive Defense** tartalmaz egy saját rendszert, melyben tárolja és kezeli a biztonsági eseményeket, hogy valós időben elemezze az összes összegyűjtött információt.

100%-BAN MENEDZSELT SZOLGÁLTATÁS

Felejtse el a műszaki személyzetbe való befektetést, akik foglalkoznak a karanténnal és a gyanús fájlokkal, vagy fertőtlenítik és helyreállítják a fertőzött számítógépeket!
Az **Adaptive Defense**, köszönhetően a Big Data környezetben lévő gépi tanulásnak, automatikusan osztályozza az összes alkalmazást, a PandaLabs szakértőinek folyamatos felügyelete mellett.

MŰSZAKI KÖVETELMÉNYEK

Web Konzol (központi kezelőfelület)

- Internet kapcsolat
- Internet Explorer 7.0 vagy újabb
- Firefox 3.0 vagy újabb
- Google Chrome 2.0 vagy újabb

Agent

- Operációs rendszerek (munkaállomások): Windows XP SP2 vagy újabb, Vista, Windows 7, 8, 8.1, és 10
- Operációs rendszerek (szerverek): Windows Server 2003, 2008, 2012 és 2016
- Internet kapcsolat (direkt, vagy egy proxy-n keresztül)