Adaptive Defense 360

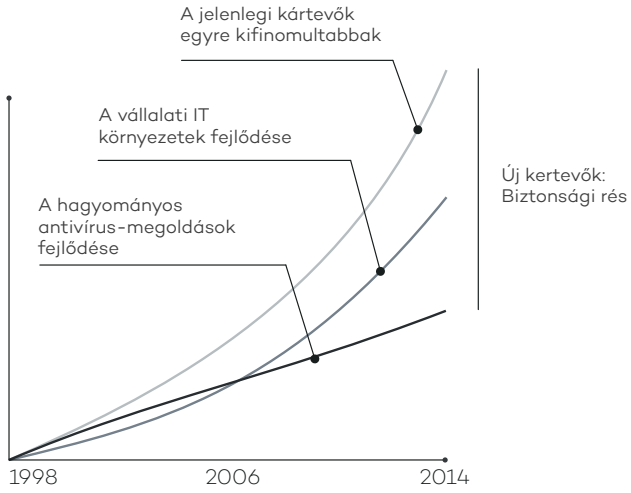
Korlátlan átláthatóság, teljes kontroll

ÁTFOGÓ VÉGPONTVÉDELMI MEGOLDÁS, AMELY MAGÁBAN FOGLALJA A VÉDELMET, A DETEKTÁLÁST, A REAGÁLÁST, VALAMINT A HELYREÁLLÍTÁST

A végpontokat nehéz megvédeni a támadásoktól. A védelemnek átfogónak kell lennie: tartalmaznia kell hagyományos vírusirtót/kártevőirtót, személyes tűzfalat, webszűrést, e-mail szűrést, valamint eszközfelügyeletet. A megoldásnak ezen felül a nehezen detektálható nulladik napi támadások (zeroday), valamint a célzott támadások ellen is védelmet kell nyújtania. A végpont teljes körű védelméhez eddig több gyártó több különböző termékére volt szükség.

Az Adaptive Defense 360 az első és egyetlen olyan termék, amely végpontvédelmet (Endpoint Protection (EPP)), valamint végponti detektálást és reagálást (Endpoint Detection & Response (EDR)) egyaránt biztosít. Az Adaptive Defense 360 automatizált képességeinek köszönhetően csökkenti az IT terheit.

Az Adaptive Defense 360 a Panda legkiemelkedőbb EPP megoldására épül, amely egyszerű és központosított biztonsági szolgáltatást, helyreállítási műveleteket, valós idejű megfigyelést és jelentéskészítést, profil-alapú védelmet, központosított eszközfelügyeletet, valamint webestartalom-figyelést és webszűrést biztosít.



Ez azonban csak a kezdet. A kártevők és az IT biztonsági környezetek egyaránt jelentős változáson mentek keresztül volumen és kifinomultság tekintetében egyaránt. Azáltal, hogy naponta több mint 200 000 új vírus jelenik meg, a védelmi rendszerek áttörésére, és a kártevő elrejtésére szolgáló technikák pedig egyre finomodnak, a vállalati hálózatok jobban ki vannak téve a nulladik napi és célzott támadásoknak, mint eddig bármikor.

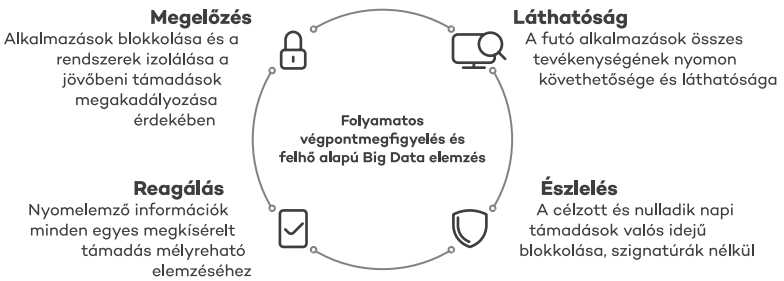
A hagyományos végpontvédelmi megoldások szignatúrákra és heurisztikus algoritmusokra épülő technikák segítségével hatékonyan blokkolják az ismert kártevőket.

Nulladik napi és célzott támadások ellen azonban nem nyújtanak védelmet, amelyek azt a biztonsági rést használják ki, amelyet az új kártevő megjelenése és a biztonsági cégek által kiadott védelmi megoldás megjelenése között eltelt idő jelent.

Ez egy egyre növekvő rés, amelyet a hackerek ki tudnak használni arra, hogy vírusokat, ransomware-eket, trójaiakat és más típusú kártevőket juttassanak a vállalati hálózatokba. Ezek az egyre gyakoribb fenyegetések titkosíthatják a bizalmas dokumentumokat és váltságdíjat követelhetnek, vagy egyszerűen érzékeny adatokat gyűjthetnek ipari kémkedés céljából.

Az Adaptive Defense a Panda megoldása az ilyen típusú támadások ellen. Az Adaptive Defense egy olyan EDR szolgáltatást biztosít, amely precízen osztályozza a szervezetnél futó összes alkalmazást, és csak a legitim programok futtatását engedélyezi.

A Panda Adaptive Defense 360 EDR szolgáltatásának biztonsági modellje 3 alapelvre épül: a vállalati számítógépeken és szervereken futó alkalmazások folyamatos megfigyelése, automatikus besorolás a felhőben működő Big Data platformunkon alkalmazott gépi tanulás (machine learning) segítségével, végül pedig az automatikusan nem besorolt alkalmazások műszaki szakértőink általi elemzése, hogy a vállalat rendszerein futó összes program viselkedését megismerjék.



Ezek a képességek egyesítésre kerültek a Panda kiemelkedő EPP megoldásával, ezzel bezárva az adaptív kártevővédelem ciklusát, amely így már magában foglalja az automatikus megelőzést, detektálást, nyomelemző információk gyűjtését, valamint a helyreállítást.

Az egyetlen megoldás, amely garantálja az összes futó alkalmazás biztonságát

GARANTÁLT TELSEJ KÖRŰ ÉS ROBUSZTUS VÉDELEM

A Panda Adaptive Defense 360 két működési módot kínál:

- A normál (standard) mód lehetővé teszi, hogy az összes goodware-ként besorolt alkalmazás fusson, azokkal az alkalmazásokkal együtt, amelyeket a Panda Security és az automatikus rendszerek még nem katalogizáltak.
- A kiterjesztett mód csak a goodware-ek futását teszi lehetővé. Ez azon vállalatok számára ideális védelmi mód, amelyeknél a legkisebb biztonsági kockázat sem megengedett.

NYOMELEMZŐ INFORMÁCIÓK

- Eseményvégrehajtási grafikonok megjelenítése a kártevő által okozott események teljes megismerése érdekében.
- Vizuális információk megjelenítése a kártevő kapcsolatok, a létrehozott fájlok és sok egyéb információ földrajzi forrásáról, hőtérképek segítségével.
- A hálózatban telepített, ismert sérülékenységekkel rendelkező szoftverek lokalizálása.

SEBEZHETŐ OPERÁCIÓS RENDSZEREK ÉS ALKALMAZÁSOK VÉDELME

Az olyan, gyártó által már nem támogatott rendszerek, mint például a Windows XP, amelyekhez már nem kerülnek kiadásra biztonsági javítások, sérülékenyek, így könnyű célpontot jelentenek a nulladik napi és az új generációs támadások számára.

Emellett a kártevők 90%-a az olyan alkalmazások sérülékenységeit használják ki, mint például a Java, Adobe, Microsoft Office, valamint a böngészők.

Az Adaptive Defense 360 sebezhetőség védelmi modulja tartalmi és viselkedési szabályokat használ annak biztosításához, hogy a vállalatok abban az esetben is biztonságos környezetben tudjanak dolgozni, ha rendszereik nincsenek megfelelően frissítve.

TELJES VÉGPONTVÉDELMI FUNKCIONALITÁS

Az Adaptive Defense 360 magába foglalja a Panda Endpoint Protection Plus-t, a Panda legkifinomultabb EPP megoldását, ezáltal teljes körű EPP funkcionalitást biztosít:

- Javító tevékenységek
- Központosított eszközfelügyelet: eszköztípusok blokkolásával megakadályozza a kártevő bejutását, valamint az adatvesztést
- Webestartalom-figyelés és -szűrés
- Vírusirtás és kéretlen levél (spam) szűrés az Exchange Szerveren
- Végponti tűzfal, és sok egyéb funkció...

FOLYAMATOS INFORMÁCIÓ A HÁLÓZATBAN LÉVŐ ÖSSZES VÉGPONT ÁLLAPOTÁRÓL

- Az eszköz azonnal riasztást küld, amikor a hálózatban kártevőt azonosít, egy átfogó jelentéssel együtt, amely tartalmazza a fertőzés helyét, a fertőzött számítógépeket, valamint a kártevő által elvégzett tevékenységeket.
- A szolgáltatás a napi tevékenységről e-mailen keresztül küld jelentést.

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

Az Adaptive Defense 360 integrálódik a SIEM megoldásokkal annak érdekében, hogy részletes információt biztosítson a rendszereken futó összes alkalmazás tevékenységéről.

SIEM megoldás nélküli kliensek esetén az Adaptive Defense 360 biztosít egy saját rendszert a biztonsági események tárolásához és kezeléséhez az összegyűjtött információk valós időben történő elemzése érdekében.

100%-BAN MENEDZSELT SZOLGÁLTATÁS

A karantén és a gyanús fájlok kezeléséhez, valamint a fertőzött gépek megtisztításához és visszaállításához nem lesz szükség a továbbiakban külön szakemberre. Az Adaptive Defense 360 a Big Data környezetben lévő machine learning segítségével automatikusan osztályozza az összes alkalmazást, a PandaLabs szakértőinek folyamatos felülvizsgálata mellette.

MŰSZAKI KÖVETELMÉNYEK

Web Konzol (központi kezelőfelület)

- Internet kapcsolat
- Internet Explorer 10
- Microsoft Edge
- Firefox (legújabb változat)
- Google Chrome (legújabb változat)

Agent

- Operációs rendszer (munkaállomás): Windows XP SP2 vagy újabb, Vista, Windows 7, 8, 8.1 és 10.
- Operációs rendszerek (szerver): Windows Server 2003 SP1 vagy újabb, 2008, 2008 R2, 2012, 2012 R2, 2016 és Server Core 2008, 2008 R2, 2012, 2012 R2 és 2016.
- Internet kapcsolat (közvetlen, vagy proxy-n keresztül)

Részlegesen támogatott (csak EPP):

- Linux, MAC OS X és Android