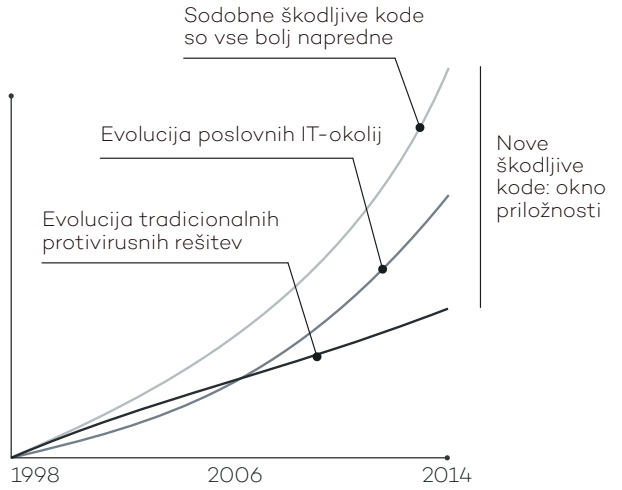
Adaptive Defense 360

Pridobite odgovore, rešite težavo

CELOVITA ZAŠČITA NAPRAV Z VGRAJENIMI MEHANIZMI ZAŠČITE, ODKRIVANJA, ČIŠČENJA IN ODZIVANJA NA VSE VRSTE GROŽENJ

Varovanje posameznih naprav pred spletnimi napadi je težka naloga. Zaščita mora vsebovati vrsto varnostnih mehanizmov, kot so protivirusni program, program za odkrivanje škodljivih kod, požarni zid, filtriranje spletnih vsebin in e-pošte ter rešitev za upravljanje naprav. A vse to še ni dovolj, potrebujemo tudi dodatno tehnologijo, ki zna naprave ščititi pred t. i. ciljanimi napadi in ranljivostmi ničtega dne (povsem sveže odkritimi luknjami). Oddelki IT so varnostne izzive do sedaj reševali predvsem z nakupom in vzdrževanjem številnih izdelkov različnih ponudnikov.

Adaptive Defense 360 pa je prva rešitev, ki ponuja zaščito naprav, funkcionalnosti odkrivanja in odzivanja na grožnje ter njihovo odpravljanje. Rešitev Adaptive Defense 360 prav tako prinaša visoko stopnjo avtomatizacije, kar posledično pomeni manjše obremenitve okolij IT. **Adaptive Defense 360** sestavljajo Pandina najboljša varnostna tehnologija zaščite naprav, preprosta in centralizirana konzola, učinkoviti varnostni ukrepi, realnočasovno spremljanje dogajanja na napravah in v omrežju ter spletno filtriranje.



Vse skupaj je šele začetek. Škodljive kode in IT-varnost so se v zadnjih letih močno spremenili – tako z vidika obsega kot vsebine. Vsak dan se v svetu pojavi več kot 200.000 novih virusov in škodljivih kod, ki znajo prelisičiti varnostne rešitve, se skriti na napravah in v omrežjih, zato so ta še bolj ranljiva na ciljane napade in napade ničtega dne.

Tradicionalne rešitve zaščite naprav, ki škodljive kode blokirajo glede na podpisne vzorce in hevristične algoritme, so le omejeno učinkovite. Žal ne ščitijo pred povsem novimi škodljivimi kodami in ciljanimi napadi, kar napadalci spretno izkoriščajo (glej sliko in okno priložnosti).

Podjetja in posameznike napadajo v času, ko za nove grožnje še ne obstajajo varnostni podpisi. To okno vse pogosteje izkoriščajo hekerji, ki svoje škodljive kode, programe za odkupnine, trojance in druge viruse podtikajo v omrežja podjetij. S temi grožnjami, ki kriptirajo dokumente in datoteke, lahko zahtevajo odkupnino ali pa zgolj zbirajo občutljive podatke z namenom industrijskega vohunjenja.

Adaptive Defense je Pandina rešitev zoper tovrstne napade. Rešitev Adaptive Defense zna zaznati tudi še neznane grožnje in jih zaustaviti. Vsako kodo in aplikacijo preveri in v poslovnem okolju omogoča le zagon varnih rešitev. Tehnologija **Panda Adaptive Defense 360** temelji na varnostnem konceptu, sestavljenem iz treh temeljnih predpostavk: stalnega nadzora aplikacij na računalnikih in strežnikih, samodejnega razvrščanja groženj ob pomoči strojnega učenja na izjemno veliki bazi podatkov v oblaku ter dodatni analizi obnašanja škodljivih kod s strani Pandinih inženirjev (tistih, za katere samodejno razvrščanje ni ugotovilo, ali so 100% varne).

Te zmogljivosti so združene z najboljšo Pandino rešitvijo za zaščito posameznih naprav, zato je varnostni krog sklenjen. Poleg stalnega preverjanja za morebitnimi napadi in njihovega preprečevanja rešitev morebitne okužbe hitro odpravi, skrbniku pa postreže s podrobnimi podaki o škodljivi kodi ali napadalcu.

EDINA REŠITEV, KI JAMČI VAROVANJE VSEH DELUJOČIH APLIKACIJ

ZAJAMČENA CELOVITA IN ROBUSTNA REŠITEV

Panda Adaptive Defense 360 pozna dva načina delovanja:

- **V standardnem načinu dovoli** izvajanje vseh aplikacij, ki jih prepozna kot varne, in aplikacij, ki so trenutno še v preverjanju pri Panda Security in drugih avtomatiziranih sistemih.
- **Naprednejši način pa omogoča** zgolj poganjanje zaupanja vrednih aplikacij. Predstavlja idealno obliko zaščite, saj ne sprejema nobenih varnostnih tveganj.

FORENZIČNE INFORMACIJE

- **Preverite, kaj so škodljive kode počele** v vašem omrežju ali sistemu.
- Vizualni prikaz informacij, tudi na zemljevidu lokacij o povezovanju škodljivih kod, okuženih datotekah itd.
- Odkiranje ranljive programske opreme v omrežju podjetja.

ZAŠČITA RANLJIVIH OPERACIJSKIH SISTEMOV IN APLIKACIJ

Sistemi, kot je Windows XP, niso več podprti s strani razvijalcev, zato so še bolj ranljivi in pogosteje tudi tarče škodljivih kod in nove generacije napadov.

Dodatno tudi ranljivosti v programski opremi, kot so Java, Adobe, Microsoft Office in praktično vsi brskalniki, predstavljajo kar 90 odstotkov tarč med škodljivimi kodami.

Modul zaščite ranljivosti v rešitvi **Adaptive Defense 360** uporablja kontekstualno učenje in pravila obnašanja, s katerimi zagotovi varno poslovno okolje podjetja, tudi če njegovi strežniki niso posodabljani.

ZAŠČITA VSEH NAPRAV

Adaptive Defense 360 ima integrirano rešitev Panda Endpoint Protection Plus, najbolj napredno rešitev zaščite naprav, ki nudi tudi funkcionalnosti:

- čiščenja okužb
- centraliziranega nadzora naprav (prepreči dostop do omrežja okuženim napravam)
- spletnega nadzora in filtriranja
- spremljanja elektronske pošte (strežnik Exchange)
- požarnega zidu in še veliko več ...

STALNO PREVERJANJE STANJA NAPRAV IN OMREŽJA

Skrbnik IT je takoj obveščen, če se v omrežju ali na napravi pojavi škodljiva koda. Rešitev mu postreže s podrobnim poročilom, vključno z lokacijo, številom okuženih naprav in aktivnostmi škodljive kode.

Prav tako lahko rešitev dnevno pošilja poročila o aktivnostih v IT-okolju.

MOŽMOST SODELOVANJA S SISTEMI ZA OKRIVANJE VDOROV

Adaptive Defense 360 se lahko integrira s sistemi za odkrivanje vdorov (SIEM) in nudi natančno spremljanje vseh delujočih aplikacij. Podjetja, ki že uporabljajo rešitev SIEM, lahko **Adaptive Defense 360** še nadgradi z lastnim sistemom za shranjevanje in upravljanje ter realnočasovno analizo varnostnih dogodkov.

100% UPRAVLJANA STORITEV

Pozabite na naložbe v tehnično osebje, ki se bo ubadalo s sumljivimi datotekami in čiščenjem okužb ter obnovo okuženih računalnikov. **Adaptive Defense 360** samodejno razvršča vse aplikacije s pomočjo strojnega učenja, v navezi z ogromnimi količinami podatkov in nadzorom s strani strokovnjakov PandaLabs pa omogoča hitro čiščenje okužb.

TEHNIČNE ZAHTEVE

Spletna konzola (le za nadzor)

- internetna povezava
- Internet Explorer 7.0 ali novejši
- Firefox 3.0 ali novejši
- Google Chrome 2.0 ali novejši

Aplikacija

- operacijski sistemi (delovne postaje): Windows XP SP2 ali novejši (Vista, Windows 7, 8, 8.1 in 10)
- operacijski sistemi (strežniki): Windows 2003 Server, Windows 2008, Windows Server 2012
- internetna povezava (direktna ali preko proxy strežnika)

Delna podpora (naprav):

- operacijski sistemi Linux, MAC OS X in Android