# Panda Patch Management

**Zmanjšajte tveganja in kompleksnost, povezane z upravljanjem in krpanjem ranljivosti v sistemih in aplikacijah najrazličnejših ponudnikov.**

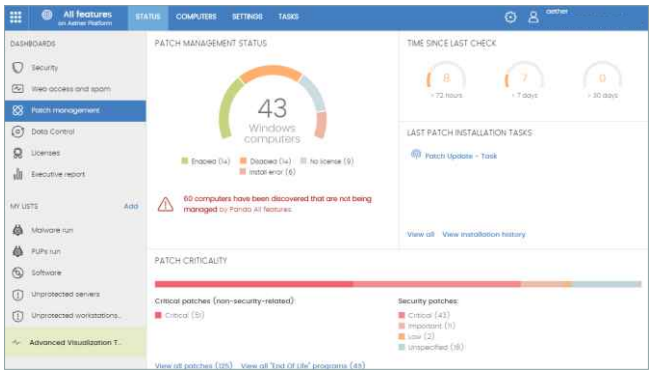
99,96 % aktivnih ranljivosti se danes nahaja v napravah v podjetjih in so posledica manjkajočih posodobitev strojne ali programske kode. Nameščene posodobitve bi močno zmanjšala varnostna tveganja. Poleg tega 86 % naprav v podjetjih nima nameščenih kritičnih popravkov aplikacij različnih ponudnikov, kot so Java, Adobe, Mozilla, Firefox, Chrome, Flash in OpenOffice[1].

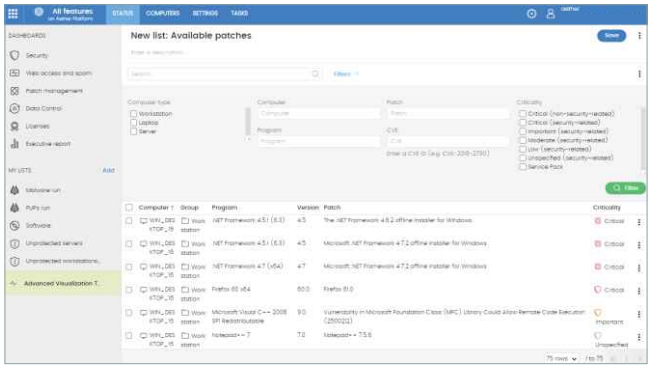
Ob nadaljevanju tega trenda bo do leta 2020 kar 99 % ranljivosti, ki povzročajo varnostne incidente, znanih vnaprej, torej bi se tem bilo mogoče zlahka izogniti, če bi naprave in programsko opremo redno posodabljali[2].

## OBVLADAJTE POSODOBITVE S PANDA PATCH MANAGEMENT

Panda Patch Management je uporabniku prijazna rešitev za upravljanje ranljivosti operacijskih sistemov in aplikacij različnih ponudnikov na delovnih postajah in strežnikih s sistemi Windows. Rešitev zmanjšuje varnostna tveganja, hkrati pa krepi obrambno sposobnost vaše organizacije, da se ubrani pred kibernetskimi in drugimi napadi.

Rešitev ne zahteva uvajanja novih naprav, programskih odjemalcev ali konzole za upravljanje, saj se popolnoma integrira v vse rešitve Panda Security. Poleg tega zagotavlja centraliziran in realno-časovni vpogled v stanje ranljivosti programske opreme, manjkajočih popravkov, posodobitev in nepodprte programske opreme (EOL3) znotraj in zunaj korporativnega omrežja. Del rešitve so tudi enostavna orodja za celovito upravljanje popravkov: od odkrivanja in načrtovanja do namestitve in spremljanja.




## RANLJIVOSTI: SKRITA TVEGANJA

Neposodobljeni **operacijski sistemi in programska oprema** različnih ponudnikov so odlična priložnost za napadalce in škodljive kode, da izkoristijo znane ranljivosti, za katere so bili sicer popravki na voljo tedne ali celo mesece pred vdorom ali napadom.

**Velika razkritja informacij** o različnih ranljivostih, npr. luknje, ki jih je izpostavila skupina Shadow Brokers ali WikiLeaks, s podrobnimi navodili glede ogrožanja sistemov in aplikacij, omogočajo pripravo napadov vedno večjemu številu profesionalnih kiberkriminalcev.

**Digitalna preobrazba**, ki s seboj prinaša vedno večje število »digitalnih« uporabnikov, naprav, sistemov in aplikacij, ki zahtevajo posodobitve, napadalcem daje na voljo vedno več tarč.

Vsaj pet skupnih izzivov otežuje boj podjetij z upravljanjem ranljivosti:

- **Postopek odkrivanja ranljivosti traja dolgo časa**. Vendar pa mora biti v primeru zaznanega incidenta odziv takojšen.
- **Podjetja so decentralizirana**, zaposleni se v omrežje podjetja povezujejo občasno. Klasična orodja za odkrivanje ranljivosti teh scenarijev ne podpirajo.
- Večina orodij za odkrivanje ranljivosti zahteva **namestitev dodatnega programa** na napravah, ki so že sicer preobremenjene.
- Orodje Microsoft VM tool organizacijam ne omogoča, da bi posodabljale **programe tretjih ponudnikov** na centraliziran in enoten način.
- Druge varnostne rešitve, ki ponujajo upravljanje popravkov, **ne povezujejo odkrivanja z odzivom v primeru ranljivih naprav**, čeprav bi to pohitrilo odziv in zajezilo obseg napada.

1 Vir: National Vulnerability Database. Kritične posodobitve aplikacij tretjih ponudnikov se samodejno nameščajo le v 14 % naprav in strežnikov v poslovnih okoljih.
2 Vir: Gartner: How to Respond to the 2018 Threat Landscape. Greg Young. Objavljeno: 28. november 2017
3 EOL (End-of-Life): Oznaka za izdelek, ki je na koncu življenjske dobe (z vidika prodajalca). Morda ne prejema več varnostnih posodobitev.

# Panda Patch Management

## PREDNOSTI

Panda Patch Management v eni sami in **do uporabnika prijazni rešitvi omogoča**:

- **Pregled, nadzor in določanje prednostnih nalog posodabljanja operacijskih sistemov in aplikacij.** Enoten pregled nad stanjem posodobitev in popravkov vsak trenutek omogoča vpogled v stanje varnosti organizacije glede na aktualne ranljivosti, popravke in čakajoče posodobitve sistemov in na stotine drugih aplikacij.
- **Preprečuje incidente, saj potencialnim napadalcem sistematično zmanjšuje površino področja**, ki ga ustvarja ranljivost programske opreme. Nudi upravljanje popravkov in posodobitev s preprostimi orodji za upravljanje v realnem času, ki organizacijam omogočajo, da ranljivosti odpravijo še pred napadom.
- **S takojšnjimi posodobitvami zajezi in ublaži napade**, ki izkoriščajo različne ranljivosti. Konzola Panda Adaptive Defense 360 v navezi z rešitvijo Patch Management organizacijam omogoča ugotavljanje povezav med odkrivanjem groženj in skritimi ranljivostmi. Odzivni čas je minimiran, rešitev napade zajezi in odpravlja tako, da iz spletne konzole takoj potiska zahteve za namestitev popravkov, čim so ti na voljo. Dodatno lahko prizadete naprave loči od preostalega omrežja in tako prepreči širjenje napada.
- **Zniža stroške poslovanja.**
- **Panda Patch Management ne zahteva uvajanja ali posodobitve novih ali obstoječih varnostnih rešitev**, obenem pa poenostavi upravljanje naprav pri čemer se izogiba preobremenitvam strežnikov in delovnih postaj.
- **Zmanjša zahtevnost nameščanja popravkov in posodobitev**, saj jih zaganja oddaljeno – iz konzole v oblaku. Takšna namestitev je dodatno optimizirana za zmanjšanje napak.
- **Takoj po aktivaciji zagotavlja popoln vpogled v vse ranljivosti**, posodobitve v teku in aplikacije, za katere podpora ni več na voljo (EoL3).
- **Upošteva načelo odgovornosti, ki ga predvidevajo številni predpisi** (GDPR, HIPAA in PCI). Organizacije prisili, da sprejmejo ustrezne tehnične in organizacijske ukrepe za zagotovitev ustrezne zaščite občutljivih podatkov, ki jih premorejo ali obdelujejo.


**Panda Patch Management pomnoži sposobnosti zaščite, odkrivanja in odzivanja, ki jih nudijo rešitve Panda Security, saj omogoča zanesljivo uvedbo koncepta prilagodljive varnostne arhitekture.4**

## KLJUČNE LASTNOSTI

Panda Patch Management nudi vsa potrebna orodja za upravljanje varnostnih popravkov in posodobitev operacijskega sistema in aplikacij tretjih ponudnikov z ene konzole:

**Celovit vpogled:**

Realnočasovni vpogled v ranljive računalnike, posodobitve na čakanju in nepodprto programsko opremo (EOL3) skupaj z načrtom posodobitev na enem mestu.

- Podrobne informacije o popravkih in čakajočih posodobitvah, podrobnosti o povezanih varnostnih biltenih ter informacije o posameznih računalnikih in ali skupinah računalnikov itd. Uporabne možnosti:

  - Filtriranje in iskanje popravkov glede na »kritičnost«, računalnik, skupino naprav, aplikacijo, vrsto popravka, oznako popravka in trenutno stanje.

  - Možnost nastavitev neposredno na računalniku: ponovni zagon, takojšnja namestitev ali namestitev z zamikom.
- Nastavljiva opozorila ob odkritju ranljivih delovnih postaj ali strežnikov.
- Samodejno iskanje posodobitev v realnem času ali v periodičnih intervalih (3, 6, 12 ali 24 ur).
- Ob odkritju aktivne škodljive kode prikaz obvestila o popravkih na čakanju. Sposobnost takojšnje namestitev popravka iz konzole, po potrebi je možno tudi izoliranje računalnika.

**Načrtovanje namestitve popravkov in posodobitev:**

- Nastavljivo glede na kritičnost in aplikacijo.
- Nastavljivo za posamezno napravo ali skupino naprav.
- Takojšnje ali načrtovano po urniku za enkratno izvedbo ali za ponovljeno izvajanje v rednih časovnih intervalih (datum/ura).
- Možnost nadzora ponovnega zagona računalnika (in določanje izjem).

**Nadzor stanja posodobitev na napravah preko:**

- Nadzorne plošče ali seznama opravil.
- Podrobnih poročil.
- Seznama posodobljenih računalnikov ter računalnikov s čakajočimi posodobitvami z napakami.

**Podrobno upravljanje na podlagi skupin in vlog z različnimi dovoljenji:**

- Glede na ranljive računalnike, popravke in servisne pakete.

**Združljivo z naslednjimi rešitvami na platformi Aether:**

Panda Endpoint Protection | Panda Endpoint Protection Plus
Panda Adaptive Defense | Panda Adaptive Defense 360

**Podprti operacijski sistemi: Windows XP SP3 ali novejši, Windows Server 2003 (32/64-bit in R2) SP2 ali novejši**

**Seznam podprtih aplikacij tretjih ponudnikov:**
https://www.pandasecurity.com/business/PatchManagementApp

### Certifikati in nagrade:

Panda Security redno sodeluje na preizkusih varnostnih rešitev s strani organizacij Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs in prejema številne nagrade. Panda Adaptive Defense je prejela certifikat EAL2+ pri ocenjevanju za standard Common Criteria.

»Gartner je podjetje Panda Security označil kot vizionarja v svojem magičnem kvadrantu platform za zaščito naprav (EPP) za leto 2018«
https://www.pandasecurity.com/gartner-magic-quadrant/

4 Vir: Gartner: "Designing an Adaptive Security Architecture for Protection from Advanced Attacks", Neil MacDonald, Peter Firstbrook