

Branite mrežu uz najbezbednije štampače kompanije HP¹



Ugrađene HP Enterprise bezbednosne funkcije za štampanje

HP Enterprise uređaji imaju ugrađene bezbednosne funkcije za automatski oporavak. Uz zaštitu ulaganja koju pruža HP FutureSmart firmver, neke funkcije možete da dodate mnogim postojećim modelima HP Enterprise štampača.¹

¹ Najnaprednije HP funkcije ugrađene sigurnosti dostupne su na uređajima klase HP Enterprise sa firmverom FutureSmart 4.5 ili novijim i zasnovane su na HP pregledu funkcija ugrađene sigurnosti objavljenih 2016-2017. na štampačima kompanije HP te klase. HP nudi kombinaciju bezbednosnih funkcija za proveru integriteta sve do BIOS-a, uz mogućnosti automatskog oporavka. Listu kompatibilnih proizvoda potražite na adresi hp.com/go/LJCompatibility.

² HP JetAdvantage Security Manager mora da se kupi zasebno. Da biste saznali više, posetite lokaciju hp.com/go/securitymanager.

Zaštita, otkrivanje i oporavak

HP štampači imaju odlične bezbednosne funkcije, sa četiri ključne tehnologije koje su uvek na oprezu i neprestano otkrivaju i sprečavaju pretnje i prilagođavaju se novima. HP Enterprise štampači automatski se oporavljaju od napada ponovnim pokretanjem – Nije neophodna intervencija IT stručnjaka.¹

Nakon ponovnog pokretanja, HP JetAdvantage Security Manager automatski procenjuje i, ako je neophodno, popravlja bezbednosna podešavanja uređaja tako da budu u saglasnosti sa ustanovljenim smernicama kompanije.² Administratori mogu da dobijaju obaveštenja o bezbednosnim događajima putem alatki za informacije o bezbednosti i upravljanje događajima (SIEM) kao što su ArcSight, Splunk i SIEMonster.

HP Sure Start – proverava radni kôd

BIOS je skup instrukcija za pokretanje koje se koriste pri učitavanju važnih hardverskih komponenti i pokretanju firmvera. Tehnologija HP Sure Start radi u pozadini tako što proverava integritet BIOS-a pri pokretanju. Ako se otkrije da je verzija ugrožena, uređaj se ponovo pokreće koristeći bezbednu, „zlatnu kopiju“ BIOS-a.

Dodavanje na belu listu – proverava autentični firmver, sa digitalnim potpisom kompanije HP

Pošto ugroženi firmver može da izloži celu vašu mrežu napadu, dodavanje na belu listu pomaže da osigurate da niko nije menjao kôd koji koordiniše funkcije, kontrole i bezbednost štampača. Firmver se automatski proverava prilikom pokretanja i, ako se otkrije neka anomalija, uređaj se ponovo pokreće u bezbednom, vanmrežnom stanju i obaveštava se IT.

Otkrivanje upada tokom rada – nadgleda aktivnost memorije

HP otkrivanje upada tokom rada pomaže da se štampači zaštite dok su uključeni i povezani sa mrežom – kada i dolazi do većine napada. Ta tehnologija proverava da li postoje anomalije tokom složenih operacija firmvera i memorije, automatski sprečava napad i ponovo pokreće uređaj.

HP Connection Inspector – proverava mrežne veze

Sprečava malver da „poziva“ zlonamerne servere, krađe podatke i ugrožava vašu mrežu. HP Connection Inspector proverava odlazne mrežne veze da bi utvrdio šta je normalno ponašanje, sprečio sumnjive zahteve i automatski ponovo pokrenuo uređaj radi oporavka.

Saznajte više: hp.com/go/PrintersThatProtect

Kako to funkcioniše?

Funkcije ugrađene sigurnosti za automatski oporavak usmerene su na četiri osnovna koraka u ciklusu HP Enterprise uređaja.

HP JetAdvantage Security Manager izvršava ciklus provere.

Četiri. Neprekidno nadgledanje

Otkrivanje upada pri radu

Nadgleda aktivnost memorije kako bi se neprekidno otkrivali i sprečavali napadi.

HP Connection Inspector

Pregleda odlazne mrežne veze kako bi se sprečili sumnjivi zahteve i zaustavio malver.

Tri. Provera postavki štampača

HP JetAdvantage Security Manager

Nakon ponovnog pokretanja proverava i popravlja sva ugrožena bezbednosna podešavanja uređaja.

Automatsko ponovno pokretanje

Jedan. Provera radnog koda

HP Sure Start

Proverava BIOS kôd i, ako je on ugrožen, ponovo pokreće sistem sa bezbednom „zlatnom kopijom“.

Dva. Provera firmvera

Dodavanje na belu listu

Proverava firmver tokom pokretanja da bi utvrdio da li je kôd autentičan – sa digitalnim potpisom kompanije HP.