Brief tehnic

Protejează-ți rețeaua cu cele mai sigure imprimante HP[1]

Funcții HP pentru securitatea imprimării

Protejează, detectează și repară

Ultima generație de dispozitive HP Enterprise este unică pe piață, pentru că oferă trei tehnologii cheie, proiectate ca împreună să contracareze eforturile atacatorilor și a se auto-repara. Aceste opțiuni declanșează automat o repornire în eventualitatea unui atac sau anomalie.

După o repornire, HP JetAdvantage Security Manager evaluează automat și, dacă este nevoie, corectează setările de securitate ale dispozitivului pentru ca acesta să fie conform cu politicile prestabilite ale companiei.[2] Nu e nevoie de intervenția departamentului IT. Administratorii pot primi notificări prin intermediul aplicațiilor HP pentru management, cum ar fi JetAdvantage Security Manager și ArcSight.

HP Sure Start

BIOS-ul este un set de instrucțiuni folosit pentru a încărca componentele fundamentale de hardware și a iniția firmware-ul HP FutureSmart al unui dispozitiv HP de clasă enterprise. Tehnologia HP Sure Start funcționează pe fundal când dispozitivele sunt pornite — protejându-ți dispozitivul de imagistică și imprimare împotriva unui atac. HP Sure Start validează integritatea codului BIOS la fiecare ciclu de pornire. Dacă este descoperită o versiune compromisă, dispozitivul repornește folosind o „copie de aur" sigură a BIOS-ului.

Procedura whitelisting

Dispozitivele HP de clasă enterprise vin cu firmware FutureSmart. La fel ca sistemul de operare al unui PC, firmware-ul coordonează funcțiile hardware, controlează panoul de control, stabilește ce opțiuni sunt disponibile când se imprimă, se scanează sau se trimit e-mailuri și protejează rețeaua. Firmware-ul compromis îți poate expune dispozitivul și rețeaua unui atac. Procedura whitelisting se asigură că doar codul autentic, recunoscut de HP — semnat digital de HP — și care nu a fost falsificat, este încărcat în memorie. Dacă se detectează o anomalie, dispozitivul repornește în stare offline securizată și așteaptă ca un firmware validat să fie încărcat. Apoi trimite o notificare către departamentul IT pentru a reîncărca firmware-ul.

Detectarea intruziunilor în timpul de funcționare

Nu ți-ai lăsa computerul neprotejat. Cu toate acestea, puțini furnizori oferă acest nivel de bază de protecție pentru dispozitivele lor de imagistică și imprimare.[1] Detectarea HP a intruziunilor în timpul de funcționare te ajută să îți protejezi dispozitivele când sunt operaționale și conectate la rețea — chiar atunci când majoritatea atacurilor au loc. Această opțiune detectează anomaliile din timpul operațiunilor complexe de firmware și memorie. În eventualitatea unui atac, dispozitivul repornește automat.

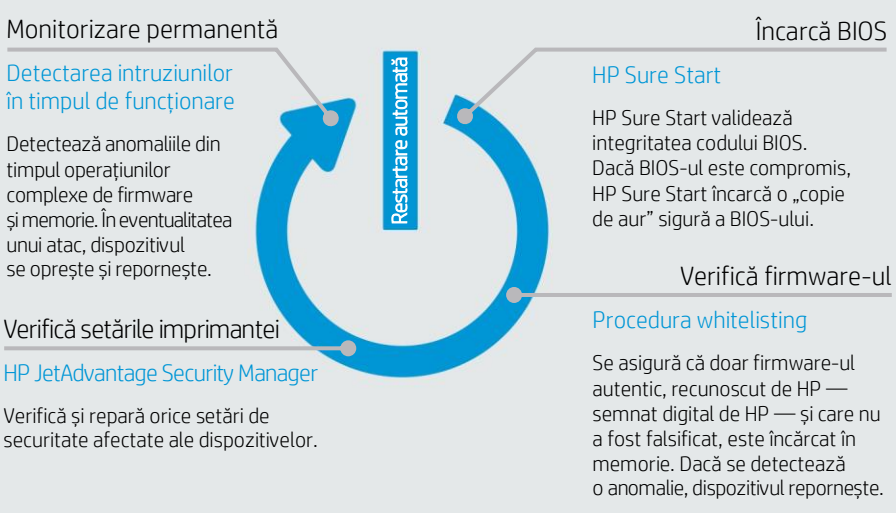
Află mai multe: hp.com/go/PrintersThatProtect

[1] Este posibil ca pentru activarea funcțiilor de securitate să fie necesară o actualizare FutureSmart a pachetului de servicii. Unele opțiuni vor fi disponibile ca parte a actualizării pachetului de servicii HP FutureSmart al anumitor imprimante Enterprise. Pentru o listă de modele compatibile, accesează hp.com/go/LJCompatibility.
[2] HP JetAdvantage Security Manager se cumpără separat. Pentru a afla mai multe, accesează hp.com/go/securitymanager.

Cum funcționează?

Opțiunile de securitate încorporate se ocupă de cei trei pași principali în ciclul de funcționare al unui dispozitiv HP.

HP JetAdvantage Security Manager completează ciclul de verificare.



Înscrie-te pentru noutăți
hp.com/go/getupdated

4AA6-1167ROE, februarie 2016