

Acronis Active Protection™

Un instrument puternic împotriva atacurilor ransomware, care vă ajută să vă protejați datele de această nouă amenințare nefastă asupra datelor

Ce este Ransomware?

Ransomware este un tip de malware deosebit de periculos. Malware-ul este un software ostil sau intruziv care este introdus ilegal pe computerul dvs. având scop dăunător și distructiv. Când ransomware-ul infectează computerul, acesta blochează accesul la datele dvs. până când îi plătiți pe infractorii care v-au atacat. În concluzie, este o amenințare ilegală și distructivă asupra datelor și informațiilor dvs.

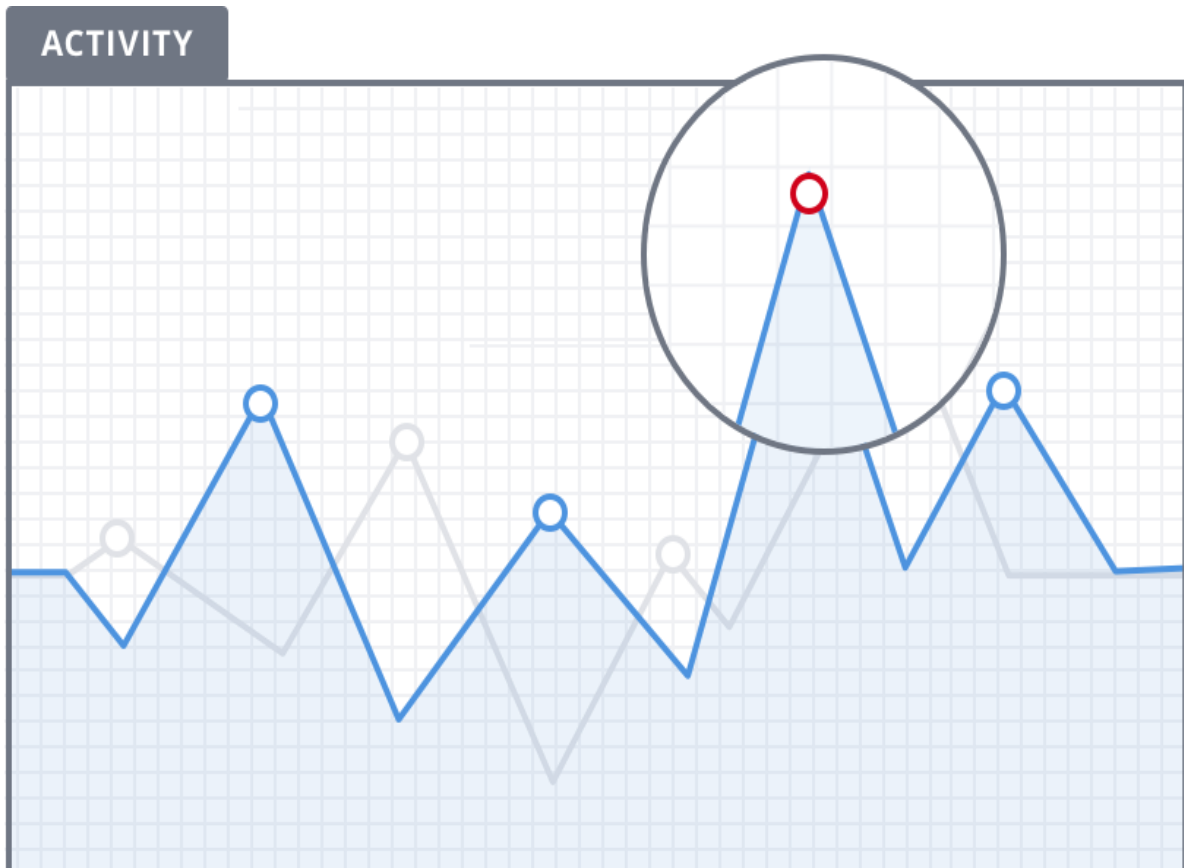
Cum funcționează Acronis Active Protection™?

Acronis Active Protection este o tehnologie avansată de protecție împotriva ransomware. Protejează în mod activ toate datele de pe computer - documente, date de toate tipurile și fișierele de rezervă Acronis. Aceasta este în prezent o caracteristică numai pentru Windows.

Funcția “Pattern detection”

Acronis Active Protection observă constant pattern-urile legate de modul cum fișierele de date se modifică pe un computer. Un set de comportamente poate fi tipic și așteptat. Un alt set de comportamente poate semnaliza un proces suspect, realizând o acțiune ostilă împotriva fișierelor. Acronis analizează aceste acțiuni și le compară cu modelele de comportament malware. Această abordare poate fi extrem

de puternică în identificarea atacurilor de ransomware/răscumpărare, chiar și în cazul variantelor de ransomware care sunt noi – nestudiate în prealabil.

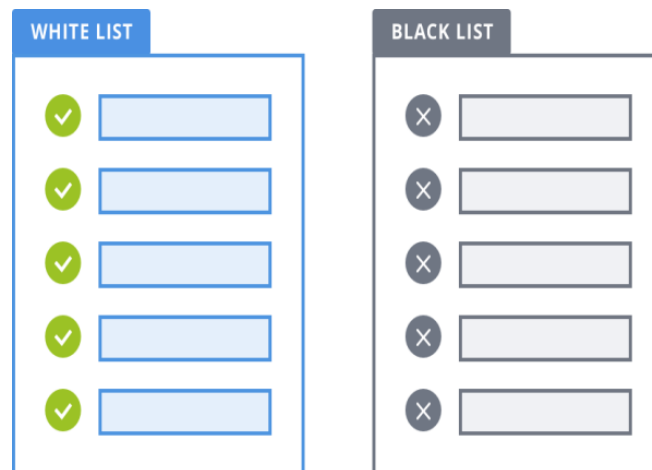


Whitelist and blacklist

Acronis Active Protection este capabil să detecteze noi amenințări bazate pe modele deja identificate – prin comparație, precum și pe cele învățate în prealabil.

Rezultatele trebuie ajustate și analizate pentru a reduce detectarea falsă a acțiunilor care până la urmă nu sunt ransomware.

Astfel, Acronis Active Protection menține o listă albă - programele care sunt permise și se așteaptă să efectueze anumite acțiuni - pentru a împiedica ca activitățile autorizate să fie etichetate din greșeală ca neautorizate.



Auto-apărarea fișierelor backup

O modalitate prin care criminali ar putea alege să compromită fișiere ar fi să atace programul Acronis True Image în sine pentru a corupe fișierele de backup create. Pentru a proteja împotriva acestui lucru, Acronis a implementat un mecanism robust de autoapărare care nu va permite infractorilor să perturbe activitatea aplicației Acronis sau a conținutului fișierelor copie de rezervă, imagine sistem, etc.

În plus, Acronis Active Protection monitorizează înregistrarea de boot master a computerelor Windows. Nu va permite efectuarea de modificări ilegale pentru a vă împiedica să încărcați corect calculatorul.



" Noua generație Acronis True Image 2017 a fost singura soluție de backup care a reușit să oprească atacurile de tip ransomware."

THE INDEPENDENT IT SECURITY INSTITUTE AV TEST REVIEW



Recuperarea efectivă a fișierelor infectate de atacul ransomware

Dacă ransomware-ul începe să cripteze fișiere, Acronis detectează și oprește rapid acest proces. Deoarece Acronis este o soluție de backup, orice date care au fost expuse și criptate înainte de oprirea procesului pot fi recuperate dintr-o varietate de surse de rezervă. Nu numai că soluțiile alternative anti-ransomware nu pot încheia un atac după ce au început, dar nu au nici o modalitate de a recupera fișierele criptate de atac. Acronis True Image cu Acronis Active Protection detectează, înlătură și restabilește fișiere de orice dimensiune!

Protecția împotriva amenințărilor viitoare

Metodologiile din Acronis Active Protection detectează, deflectă și restaurează în mod avansat. Aceste abordări de protecție nu numai că stau în fața criminalilor, dar

sunt mai inovatoare și mai avansate decât orice altă metodă anti-ransomware disponibilă. Soluția vine să vă protejeze împotriva:

- Atacatorilor care încearcă să vă infecteze sau vă să compromită backup-ul local sau salvat în cloud.
- Atacurilor care sunt mai mici (dar periodice) și mai greu de observat, de exemplu schimbă doar o mică parte dintr-un document sau doar o fotografie din mai multe de pe hard disk.
- Atacatorilor care vin mereu cu noi modalități creative în încercarea nefastă de vă schimba/cripta fișierele fără știrea dvs.