



**Bitdefender**<sup>®</sup>

**Endpoint Security for  
Mac**

**MANUAL DE UTILIZARE**

## Endpoint Security for Mac Manual de utilizare

Publicat 2020.08.31

Copyright© 2020 Bitdefender

### Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reprodusă sau transmisă sub nicio formă și prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare și recuperare de date, fără acordul scris al unui reprezentant autorizat al Bitdefender. Este posibilă includerea unor scurte citate în recenzii, dar numai cu condiția menționării sursei citate. Conținutul documentului nu poate fi modificat în niciun fel.

**Avertisment și declinarea responsabilității.** Acest produs și documentația aferentă sunt protejate de legea drepturilor de autor. Informațiile incluse în acest document sunt furnizate „ca atare”, fără nicio garanție. Deși s-au luat toate măsurile de prevedere în momentul alcătuirii acestui document, autorii săi nu vor fi în niciun fel ținuți responsabili față de nicio persoană fizică sau juridică pentru pierderi sau daune cauzate sau care se presupune a fi fost cauzate, direct sau indirect, de informațiile cuprinse în acest material.

Acest document conține legături către siteuri web aparținând unor terți, care nu se află sub controlul Bitdefender; prin urmare, Bitdefender nu este responsabilă pentru conținutul respectivelor siteuri. Responsabilitatea accesării oricăruia dintre siteurile terților a căror legătură este furnizată în acest document vă aparține în totalitate. Bitdefender furnizează aceste legături exclusiv pentru ușurarea consultării documentului și prezența lor nu presupune faptul că Bitdefender susține sau își asumă responsabilitatea pentru conținutul siteurilor către care duc acestea.

**Mărci înregistrate.** Acest document poate conține nume de mărci înregistrate. Toate mărcile comerciale înregistrate sau neînregistrate din acest document aparțin exclusiv proprietarilor acestora și sunt redată ca atare.

## Cuprins

Cum să folosiți acest ghid .....	v
1. Scopul și publicul țintă .....	v
2. Cum să folosiți acest ghid .....	v
3. Convenții utilizate în ghid .....	vi
3.1. Convenții tipografice .....	vi
3.2. Atenționări .....	vi
4. Comentarii .....	vii
1. Introducere .....	1
1.1. Despre Endpoint Security for Mac .....	1
1.2. Deschide Endpoint Security for Mac .....	1
1.3. Fereastra principală a aplicației .....	2
1.4. Pictograma aplicației din Dock .....	4
2. Protecția împotriva programelor malware .....	5
2.1. Recomandări de utilizare .....	5
2.2. Scanarea Mac-ului dumneavoastră .....	5
2.3. Asistent scanare .....	6
2.4. Remedierea problemelor .....	7
2.5. Carantină .....	9
2.6. Content Control .....	10
2.7. Device Control .....	11
2.8. Protecție web .....	12
2.9. Actualizări .....	13
2.9.1. Cererea unei actualizări .....	14
2.9.2. Obținerea actualizărilor prin intermediul unui server proxy .....	14
2.9.3. Actualizați-vă la o nouă versiune .....	14
3. Utilizarea criptării .....	15
3.1. Criptarea volumelor .....	15
3.2. Decriptarea volumelor .....	17
3.3. Modificarea cheii de recuperare .....	18
3.4. Modificarea parolei de criptare .....	19
4. Configurarea preferințelor .....	20
4.1. Accesarea preferințelor .....	20
4.2. Carantină .....	20
4.3. Istoric .....	20
4.4. Preferințe de scanare .....	21
5. Folosind instrumentul linie de comandă .....	22
5.1. Comenzi acceptate .....	22
5.2. Parametrul codului de autentificare .....	25
5.3. Coduri de eroare .....	25
6. Întrebări frecvente .....	27
7. Obținere ajutor .....	29



Tipuri de softuri periculoase ..... 30

## Cum să folosiți acest ghid

### 1. Scopul și publicul țintă

Această documentație este destinată pentru utilizatorii finali ai **Endpoint Security for Mac**, software-ul client Security for Endpoints instalat pe calculatoare pentru a le proteja împotriva programelor periculoase și a altor amenințări de pe Internet. Informațiile prezentate aici ar trebui să fie ușor de înțeles de către oricine care este capabil să lucreze cu Macintosh.

Veți afla cum să configurați și să utilizați Endpoint Security pentru Mac pentru a proteja computerul împotriva virusilor și a altor programe nocive. Veți învăța cum să obțineți cele mai bune de la Bitdefender.

Vă dorim o lectură plăcută și utilă.

### 2. Cum să folosiți acest ghid

Acest ghid este organizat în mai multe teme majore:

[Introducere \(p. 1\)](#)

Începeți cu Endpoint Security pentru Mac și interfața sa cu utilizatorul.

[Protecția împotriva programelor malware \(p. 5\)](#)

Aflați cum se utilizează Endpoint Security pentru Mac pentru a vă proteja calculatorul împotriva software-ului periculos.

[Configurarea preferințelor \(p. 20\)](#)

Aflați mai multe despre preferințele Endpoint Security pentru Mac.

[Obținere ajutor \(p. 29\)](#)

Unde să căutați și unde să cereți ajutor în cazul în care apar situații neprevăzute.

## 3. Convenții utilizate în ghid


### 3.1. Convenții tipografice


Manualul conține diferite stiluri de text, pentru o lectură cât mai ușoară. Aspectul și semnificația acestora sunt prezentate în tabelul de mai jos.

Aspect	Descriere
exemplu de sintaxă	Exemplele de sintaxă sunt tipărite cu caractere monospațiate.
<a href="http://www.bitdefender.ro">http://www.bitdefender.ro</a>	Linkurile URL indică locații externe, pe serverele http sau ftp.
<a href="mailto:documentation@bitdefender.com">documentation@bitdefender.com</a>	Adresele de e-mail sunt inserate în text ca adrese de contact.
Cum să folosiți acest ghid (p. v)	Acesta este un link intern, către o locație din document.
nume fișier	Numele fișierelor și ale directoarelor sunt tipărite cu caractere monospațiate.
opțiuni	Toate opțiunile produsului sunt tipărite cu caractere <b>bold</b> .
cuvânt cheie	Cuvintele cheie sau frazele importante sunt evidențiate cu ajutorul caracterelor <b>bold</b> .

### 3.2. Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

 **Notă**  
Nota nu este decât o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect asemănător.

 **Important**  
Acest lucru necesită atenția dumneavoastră și nu este recomandat să-l ocoliți. De obicei, aici se furnizează informații importante, dar nu cruciale.

**Avertisment**

Este vorba de informații cruciale, cărora trebuie să le acordați o mare atenție. Dacă urmați indicațiile, nu se va întâmpla nimic rău. Este indicat să citiți și să înțelegeți despre ce este vorba, deoarece aici se descrie ceva extrem de riscant.

## 4. Comentarii

Vă invităm să ne ajutați să îmbunătățim acest manual. Am testat și verificat toate informațiile, în măsura posibilităților noastre. Vă rugăm să ne scrieți despre orice inexactități pe care le veți găsi în această carte sau despre cum credeți că ar putea fi îmbunătățită, pentru a ne ajuta să vă oferim cea mai bună documentație.

Aveți la dispoziție următoarea adresă de e-mail [documentation@bitdefender.com](mailto:documentation@bitdefender.com). Vă rugăm să scrieți în engleză sau română mailurile către adresa de mai sus pentru a le putea procesa cât mai eficient.

## 1. INTRODUCERE

Acest capitol acoperă următoarele subiecte:

- [Despre Endpoint Security for Mac](#)
- [Deschide Endpoint Security for Mac](#)
- [Fereastra principală a aplicației](#)
- [Pictograma aplicației din Dock](#)

### 1.1. Despre Endpoint Security for Mac

Endpoint Security pentru Mac este un program informatic de securitate complet automat, gestionat de la distanță de către administratorul de rețea. Odată instalat, el vă protejează împotriva tuturor tipurilor de programe periculoase, inclusiv viruși, programe de tip spyware, troieni, keyloggers, viermi și adware. Acesta poate fi folosit și pentru a pune în aplicare politicile de folosire a computerului și Internetului din cadrul organizației dumneavoastră

Această aplicație detectează și elimină nu numai malware pentru Mac, ci și malware pentru Windows, împiedicându-vă, astfel, să transmiteți fișiere infectate familiei, prietenilor și colegilor care utilizează PC-uri.

### 1.2. Deschide Endpoint Security for Mac

Aveți la dispoziție mai multe moduri de a deschide Endpoint Security pentru Mac.

- Faceți clic pe icoana Security Endpoint pentru Mac în Launchpad.
- Deschideți o fereastră Finder, mergeți la **Applications** ;i faceți dublu clic pe pictograma **Endpoint Security for Mac**.
- De asemenea, puteți folosi Spotlight pentru a găsi și deschide aplicația.

Atunci când aplicația se deschide, acesta detectează automat limba sistemului și afișează interfața utilizatorului în limba dumneavoastră.



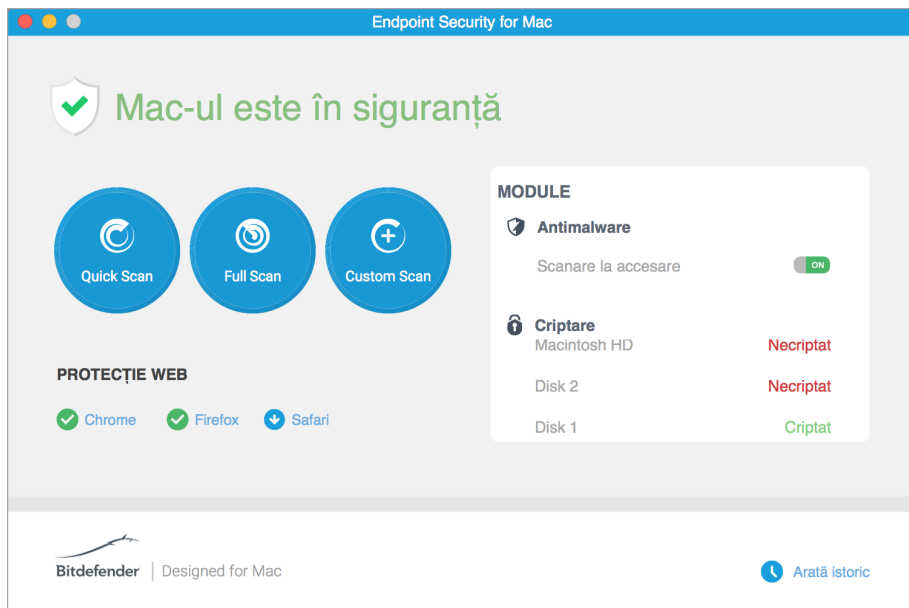
#### Notă

Dacă limba sistemului nu este printre limbile suportate de Endpoint Security for Mac, aplicația încarcă implicit interfața în limba engleză.



## 1.3. Fereastra principală a aplicației

În fereastra principală a aplicației puteți lua măsuri importante pentru a îmbunătăți protecția sistemului dvs.. Puteți verifica starea de securitate a computerului dvs. și să vă asigurați experiența de navigare web.



Fereastra principală a aplicației

Zona de stare din partea de sus a ferestrei vă informează despre starea de securitate a sistemului folosind mesaje explicite și culori sugestive:

- Verde - Dacă Endpoint Security for Mac nu are avertismente.
- Galben - Dacă a fost detectată o problemă de securitate.
- Roșu - Dacă licența a expirat.

La zona de stare, sunt disponibile trei butoane de scanare pentru a vă ajuta să scanați Mac-ul dumneavoastră:

- **Quick Scan (Scanare rapidă)** - verifică dacă există programe malware în cele mai vulnerabile locații din sistemul dumneavoastră (de exemplu, folderele care

conțin documentele, fișierele descărcate de pe web sau din e-mail și fișierele temporare ale fiecărui utilizator).

- **Full Scan (Scanare completă)** - efectuează o verificare completă a întregului sistem pentru identificarea programelor malware. Toate dispozitivele conectate vor fi, de asemenea, scanate.
- **Custom Scan (Scanare personalizată)** - vă ajută să verificați anumite fișiere, foldere sau volume pentru a identifica programele malware.

Pentru mai multe informații, consultați capitolul [Scanarea Mac-ului dumneavoastră \(p. 5\)](#).

Secțiunea pentru module, aflată lângă butoanele de scanare, vă informează despre:

- **Anti-malware** – vă informează dacă scanarea la accesare este activată (On) sau dezactivată (Off).
- **Control conținut** - vă informează dacă următoarele componente sunt activate (On) sau dezactivate (Off):
  - Scanare trafic
  - Lista neagră de aplicații
  - Control Acces Web
  - Antiphishing
- **Control dispozitive** - vă informează dacă modulul este activat (On) sau dezactivat (Off).



### Notă

Modulele Control conținut și Control dispozitive sunt disponibile începând cu OS X El Capitan (10.11). Aceste funcționalități se bazează pe o extensie de kernel macOS. Instalarea extensiilor de kernel necesită aprobarea utilizatorului pe macOS High Sierra (10.13) și versiunile ulterioare.

- **Criptare** – furnizează starea de criptare a fiecărui disc (Criptat, Criptare în curs, Decriptare în curs, Necriptat, Blocat sau Suspendat) în cazul în care pentru computerul dumneavoastră se aplică o politică de criptare.
- **EDR Sensor** - informs you if the EDR module is enabled (On) or disabled (Off).

Sub butoanele de scanare, este disponibilă o opțiune suplimentară:

- **Protecție web** - filtrează tot traficul dumneavoastră web și blochează orice conținut periculos pentru o experiență sigură de browsing web. Pentru informații suplimentare, consultați [Protecție web \(p. 12\)](#).

**Notă**

Modulul Protecție web este disponibil pe OS X Mavericks (10.9) și OS X Yosemite (10.10). Începând cu OS X El Capitan (10.11), această caracteristică este înlocuită de modulul Control conținut.

Efectuând clic pe **Vezi istoricul** din partea de jos a ferestrei, veți deschide un jurnal detaliat al evenimentelor privind securitatea stației de lucru pentru activitatea Mac pe computerul dumneavoastră. Pentru detalii, consultați [Istoric \(p. 20\)](#).

## 1.4. Pictograma aplicației din Dock

Pictograma Endpoint Security pentru Mac poate fi observată în Dock, de îndată ce deschideți aplicația. Pictograma din Dock vă oferă o modalitate ușoară de a scana fișierele și folderele de programe periculoase. Pur și simplu trageți și plasați fișierul sau dosarul pe pictograma Dock și scanarea va începe imediat.



Pictograma Dock

## 2. PROTECȚIA ÎMPOTRIVA PROGRAMELOR MALWARE

Acest capitol acoperă următoarele subiecte:

- [Recomandări de utilizare](#)
- [Scanarea Mac-ului dumneavoastră](#)
- [Asistent scanare](#)
- [Remediarea problemelor](#)
- [Carantină](#)
- [Content Control](#)
- [Device Control](#)
- [Protecție web](#)
- [Actualizări](#)

### 2.1. Recomandări de utilizare

Pentru a vă proteja sistemul de programe periculoase și pentru a preveni infectarea accidentală a altor sisteme, respectați aceste bune practici:

- Verificați și rezolvați problemele raportate de Endpoint Security pentru Mac în mod regulat. Pentru informații detaliate, consultați capitolul [Remediarea problemelor \(p. 7\)](#).
- Vă sugerăm să urmați aceste recomandări de utilizare:
  - Obișnuiți-vă să scanați fișierele pe care le descărcați de pe o memorie externă de stocare (precum un stick USB sau un CD), în special atunci când sursa nu vă este cunoscută.
  - În cazul unui fișier DMG, instalați-l și apoi scanați conținutul acestuia (fișierele din volumul/imaginea instalată).

### 2.2. Scanarea Mac-ului dumneavoastră

Modulul de scanare la accesare monitorizează permanent calculatorul dumneavoastră, căutând acțiunile de tip malware și prevenind pătrunderea în sistem a noilor amenințări. Scanarea la accesare este controlată de administratorul de rețea prin intermediul politicilor de securitate.

De asemenea, puteți scana Mac-ul dumneavoastră sau anumite fișiere oricând doriți.

Cea mai ușoară modalitate de scanare a unui fișier, folder sau volum este prin tragere și lipire (drag & drop) deasupra pictogramei Dock. Se va afișa asistentul de scanare, care vă va ghida pe parcursul procesului de scanare.

Puteți porni o scanare după cum urmează:

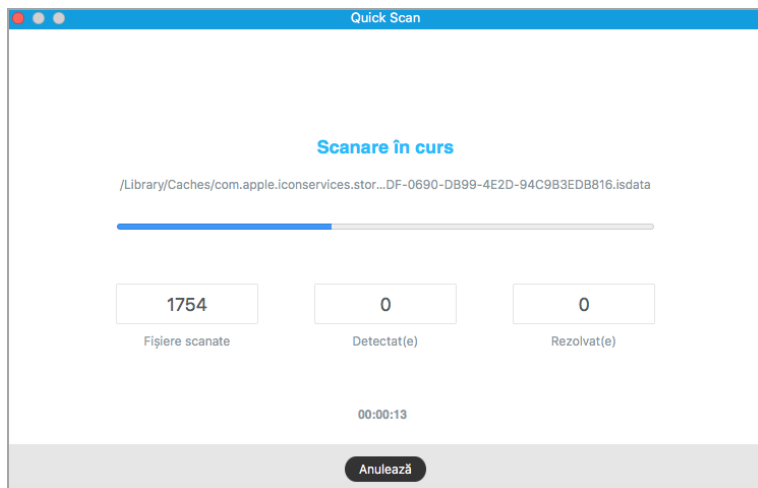
1. Deschide Endpoint Security for Mac
2. Faceți clic pe unul dintre cele trei butoane de scanare pentru a începe scanarea dorită.
  - **Quick Scan (Scanare rapidă)** - verifică dacă există programe malware în cele mai vulnerabile locații din sistemul dumneavoastră (de exemplu, folderele care conțin documentele, fișierele descărcate de pe web sau din e-mail și fișierele temporare ale fiecărui utilizator).
  - **Full Scan (Scanare completă)** - efectuează o verificare completă a întregului sistem pentru identificarea programelor malware. Toate dispozitivele conectate vor fi, de asemenea, scanate.

### Notă

- În funcție de dimensiunea hard disk-ului dumneavoastră, scanarea întregului sistem poate dura până la o oră sau chiar mai mult. Pentru o mai bună performanță, se recomandă să nu rulați această operațiune în timp ce efectuați alte operațiuni care folosesc intensiv resursele (cum ar fi editarea video).
- You can also run a quick scan or a full scan by using the **productConfigurationTool** [folosind instrumentul linie de comandă \(p. 22\)](#).
- **Custom Scan (Scanare personalizată)** - vă ajută să verificați anumite fișiere, foldere sau volume pentru a identifica programele malware.

## 2.3. Asistent scanare

Atunci când inițiați o scanare, va apărea expertul de scanare Endpoint Security pentru Mac.



Scanare în curs...

Puteți vedea în timp real informații despre scanare, cum ar fi numărul de amenințări detectate și numărul de probleme rezolvate.

Așteptați ca Endpoint Security pentru Mac să termine scanarea.



### Notă

Procesul de scanare poate dura cateva minute, în funcție de complexitatea scanării.

## 2.4. Remedierea problemelor

Endpoint Security pentru Mac detectează automat și vă informează despre o serie de probleme care pot afecta securitatea sistemului și a datelor dumneavoastră.

Problemele detectate pot face referire la:

- Noi semnături de malware și actualizări de produs nu au fost descărcate de pe serverele Bitdefender.
- În sistemul dumneavoastră au fost detectate amenințări de securitate.
- Modulul de scanare la accesare este dezactivat.
- Licența a expirat.

Remedierea problemelor indicate de Endpoint Security for Mac este un proces rapid și ușor. Astfel, puteți rezolva problemele de securitate în timp util.

Pentru a verifica și soluționa problemele detectate:

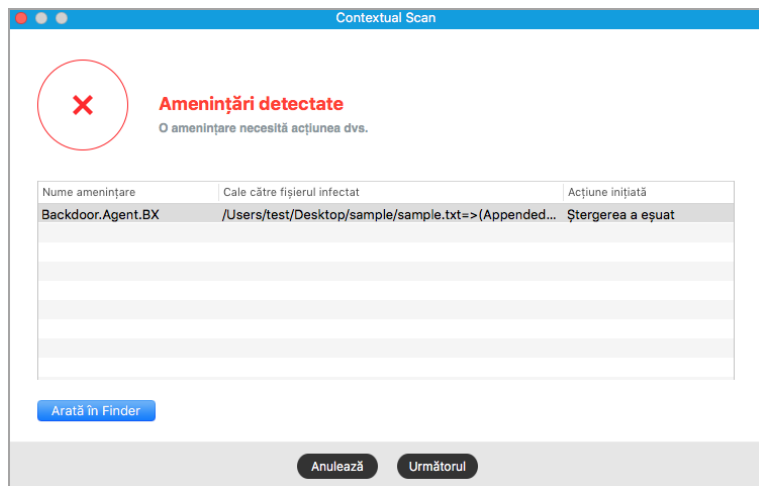
1. Deschide Endpoint Security for Mac
2. Verificați culoarea zonei de stare:
  - Verde - Mac-ul dumneavoastră este în siguranță.
  - Galben sau roșu - Mac-ul dumneavoastră prezintă probleme. Pentru mai multe investigații, urmați pașii de mai jos.
3. Verificați descrierea acestuia pentru a obține mai multe informații.
4. În funcție de numărul și tipul problemelor detectate, în zona de stare poate fi disponibil un buton:
  - **Remediază problema**, dacă a fost identificată o singură problemă. Faceți clic pe buton pentru a remedia rapid riscul de securitate.
  - **Vizualizează problemele**, dacă au fost identificate mai multe probleme. Faceți clic pe buton pentru a vizualiza problemele. Se deschide o nouă fereastră, unde puteți rezolva problemele.

Dacă s-a detectat un program malware, aplicația încearcă automat să-l șteargă și să reconstruiască fișierul inițial. Această operațiune este denumită dezinfectare. Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a menține infecția sub control.

Dacă fișierul nu poate fi nici dezinfectat, nici mutat în carantină, Endpoint Security for Mac vă informează despre această problemă și îl veți putea șterge manual.

Pentru a șterge manual fișierele infectate:

- Faceți clic pe butonul **Arată în Finder**.
  - Selectați fișierul și ștergeți-l din sistemul dumneavoastră.
- Dacă fișierul aparține unei aplicații instalate, asigurați-vă că reparați instalarea respectivă pentru ca programul să funcționeze corect.



Fereastra de amenințări nesoluționate

Este posibil ca anumite probleme să poată fi rezolvate numai de către administratorul de rețea din consola de administrare, cum ar fi:

- Activarea modulului de scanare la accesare prin intermediul politicii de securitate.
- Reînnoirea licenței expirate.

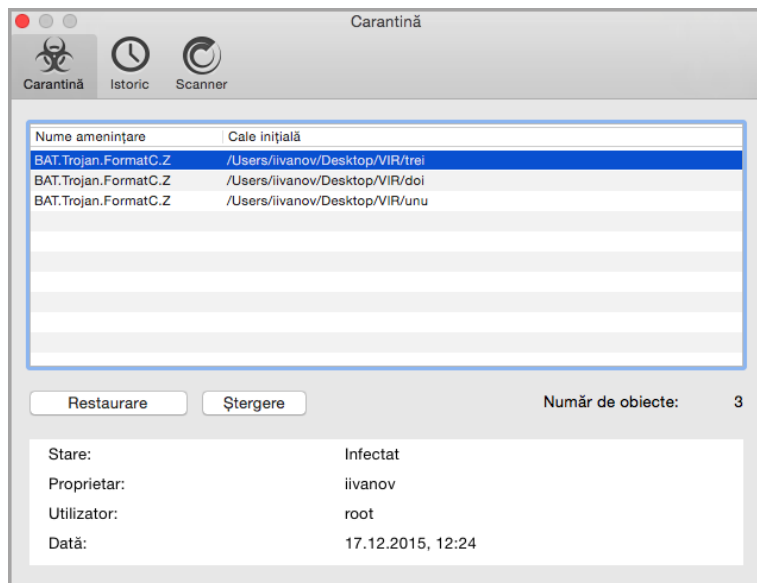
## 2.5. Carantină

Endpoint Security pentru Mac permite izolarea fișierelor infectate sau suspecte într-o zonă sigură, numită carantină. Atunci când o aplicație periculoasă este mutată în carantină, aceasta nu prezintă niciun risc, deoarece nu poate fi executată sau citită.

Pentru a vizualiza și administra fișierele din carantină, deschideți fereastra **Carantină**:

1. Dați clic dreapta pe pictograma Bitdefender din bara de meniu.
2. Selectați **Preferințe** din lista de opțiuni. Se va deschide o fereastră.
3. Selectați fila **Vizualizare carantină**.





Fișiere mutate în carantină

Secțiunea Carantină afișează toate fișierele izolate în directorul Carantină.

Pentru a șterge un fișier aflat în carantină, selectați-l și faceți clic pe **Șterge**. Dacă doriți să restaurați un fișier aflat în carantină în locația sa originală, selectați-l și faceți clic pe **Restaurează**.

## 2.6. Content Control

Modulul Control conține vă protejează împotriva atacurilor de phishing, a tentativelor de fraudă și conținutului web inadecvat atunci când navigați pe internet. Acesta include, de asemenea, o serie completă de opțiuni de control, care ajută administratorul de rețea să pună în aplicare politicile de utilizare a computerului și internetului. Acest modul este disponibil pentru Chrome, Firefox și Safari.

- **Scanare trafic.** Această componentă împiedică descărcarea de malware pe stația de lucru prin scanarea traficului web în timp real.
- **Lista neagră de aplicații.** Această componentă previne accesul la aplicațiile neautorizate din compania dumneavoastră. Administratorul este responsabil de crearea regulilor pentru aplicații în cadrul organizației.

- **Control acces web.** Această componentă vă protejează de accesarea site-urilor periculoase pe baza unor reguli definite de administrator.
- **Antiphishing.** Această componentă blochează automat paginile de phishing cunoscute pentru a împiedica utilizatorii să divulge din neatenție informații private sau confidențiale infractorilor online.

### **i** Notă

Modulul Control conținut este disponibil începând cu OS X El Capitan (10.11). Această funcționalitate se bazează pe o extensie de kernel macOS. Instalarea extensiilor de kernel necesită aprobarea utilizatorului pe macOS High Sierra (10.13). Sistemul vă notifică atunci când o extensie de sistem Bitdefender a fost blocată și vă informează că o puteți debloca din preferințele de **Securitate și confidențialitate**. Până când nu aprobați extensia de sistem Bitdefender, acest modul nu va funcționa, iar în interfața utilizatorului din Endpoint Security for Mac se va afișa o problemă critică, necesitând aprobarea dvs.

## 2.7. Device Control

Modulul **Control dispozitive** vă permite să preveniți scurgerile de date cu caracter sensibil și infectările cu malware prin intermediul dispozitivelor externe atașate stațiilor de lucru, prin aplicarea unor reguli de blocare pe bază de politică valabile pentru o gamă largă de dispozitive. Administratorul este responsabil pentru gestionarea permisiunilor pentru următoarele tipuri de dispozitive:

- Dispozitive Bluetooth
- Dispozitive CDROM
- Dispozitive de imagine
- Modemuri
- Windows portabil
- Imprimante
- Adaptoare de rețea
- Adaptoare de rețea wireless
- Stocare externă

### **i** Notă

Modulul Control dispozitive este disponibil începând cu OS X El Capitan (10.11). Această funcționalitate se bazează pe o extensie de kernel macOS. Instalarea extensiilor de kernel necesită aprobarea utilizatorului pe macOS High Sierra (10.13). Sistemul vă notifică atunci când o extensie de sistem Bitdefender a fost blocată și vă informează că o puteți debloca din preferințele de **Securitate și confidențialitate**. Până când nu aprobați extensia de sistem Bitdefender, acest modul nu va funcționa,

iar în interfața utilizatorului din Endpoint Security for Mac se va afișa o problemă critică, necesitând aprobarea dvs.

## 2.8. Protecție web

Endpoint Security pentru Mac utilizează extensiile TrafficLight pentru a asigura complet experiența de navigare web. Extensiile TrafficLight interceptează, procesează și se filtrează tot traficul web, blocând orice conținut rău intenționat.

Extensiile sunt compatibile și se integrează cu următoarele browsere web: Mozilla Firefox, Google Chrome și Safari.



### Notă

Această caracteristică este disponibilă pe OS X Mavericks (10.9) și OS X Yosemite (10.10). Începând cu OS X El Capitan (10.11), modulul Protecție web este înlocuit de modulul Control conținut.

Sunt disponibile o serie de caracteristici pentru a vă proteja de toate tipurile de amenințări cu care v-ați putea confrunța în timpul navigării pe internet:

- Filtru avansat pentru phishing - împiedică accesarea site-urilor web utilizate pentru atacuri de tip phishing.
- Filtru malware - blochează orice softuri periculoase cu care intrați în contact în timp ce navigați pe internet.
- Analizator rezultate căutare - vă avertizează în avans cu privire la site-urile web periculoase din cadrul rezultatelor căutării efectuate de dumneavoastră.
- Filtru antifraudă - asigură protecție împotriva site-urilor web frauduloase în timpul navigării pe internet.
- Notificare tracker - detectează trackerile de pe paginile web vizitate, protejându-vă confidențialitatea online.

## Activarea extensiilor TrafficLight




Pentru a activa extensiile TrafficLight, urmați pașii de mai jos:

1. Deschide Endpoint Security for Mac
2. Faceți clic pe **Remediază acum** pentru a deschide fereastra Protecție web.

3. Endpoint Security for Mac va detecta tipul de browser instalat pe sistemul dumneavoastră. Pentru a instala extensia TrafficLight pe browserul dorit, faceți clic pe **Obținere extensie** din secțiunea corespunzătoare.
4. Veți fi redirecționat la această locație online:  
<http://bitdefender.com/solutions/trafficlight.html>
5. Selectați **Descărcare gratuită**.
6. Urmați pașii indicați pentru a instala extensia TrafficLight pentru browserul web selectat.

## Rating-ul de pagină și alerte

În funcție de cum clasifică TrafficLight pagina web pe care o vizualizați la momentul respectiv, una sau mai multe dintre următoarele pictograme sunt afișate în zona corespunzătoare:

-  Este o pagină sigură. Puteți continua.
-  Această pagină poate avea conținut periculos. Procedați cu precauție dacă decideți să o accesați.
-  Ar trebui să închideți imediat această pagină web. În mod alternativ, puteți selecta una dintre următoarele opțiuni disponibile:
  - Ieșiți din site-ul web făcând clic pe **Revenire la o pagină sigură**.
  - Accesați site-ul web, în ciuda avertismentului, făcând clic pe **Înțeleg riscurile și doresc să accesez această pagină**.

## 2.9. Actualizări

În fiecare zi sunt descoperite și identificate programe periculoase noi. Acesta este motivul pentru care este foarte important să mențineți Endpoint Security pentru Mac actualizat cu cele mai recente semnături de programe periculoase.

Când **Scanarea la accesare** este activată, semnăturile de malware și actualizările de produse sunt descărcate automat în sistemul dumneavoastră. Dacă administratorul de rețea dezactivează modulul de scanare la accesare prin intermediul politicii de securitate, trebuie să solicitați manual actualizarea aplicației Endpoint Security for Mac.

Actualizarea semnăturilor de malware se efectuează din mers, adică fișierele care trebuie actualizate sunt înlocuite progresiv. Astfel, actualizarea nu va afecta funcționarea produsului și, în același timp, se elimină orice vulnerabilitate.

### 2.9.1. Cererea unei actualizări

Puteți efectua o actualizare la cerere oricând doriți. Actualizarea la cererea utilizatorului este recomandată înainte de lansarea unei scanări amânunțite.

Este necesară o conexiune activă la internet pentru a verifica dacă există actualizări disponibile și pentru a le descărca.

Pentru o actualizare la cerere:

1. Deschide Endpoint Security for Mac
2. Faceți clic pe **Actions** din bara de meniu.
3. Alegeți **Update Virus Database**.

Puteți vizualiza progresul actualizării, precum și fișierele descărcate.

### 2.9.2. Obținerea actualizărilor prin intermediul unui server proxy

Endpoint Security pentru Mac se poate actualiza numai prin servere proxy care nu necesită autentificare. Nu este necesară configurarea nici unor setări de program.

Dacă vă conectați la internet prin intermediul unui server proxy ce necesită autentificare, trebuie să treceți în mod regulat la o conexiune directă la internet pentru a putea obține actualizările semnăturilor softurilor periculoase.

### 2.9.3. Actualizați-vă la o nouă versiune

Ocazional, lansăm actualizări de produs pentru a îmbunătăți funcționalitățile produsului. Aceste actualizări pot necesita repornirea sistemului pentru a porni instalarea noilor fișiere. În mod implicit, dacă o actualizare necesită repornirea computerului, Endpoint Security pentru Mac va continua funcționarea folosind fișierele anterioare, până când reporniți sistemul. În acest caz, procesul de actualizare nu vă va afecta munca.

Atunci când este finalizată o actualizare de produs, o fereastră pop-up vă va solicita să reporniți sistemul. Dacă ratați această notificare, puteți fie să faceți clic pe **Restart to upgrade** din bara de meniu sau să reporniți manual sistemul.

### 3. UTILIZAREA CRIPTĂRII

Modulul Criptare asigură caracteristica Full Disk Encryption pe Mac-ul dumneavoastră prin intermediul politicilor aplicate de administratorul dumneavoastră de securitate. Agentul de securitate operează FileVault pentru a cripta unitatea de disc de tip boot a Mac-ului și utilitarul pe bază de linie de comandă diskutil pentru a cripta orice unitate de disc non-boot. Dispozitivele amovibile nu sunt criptate.

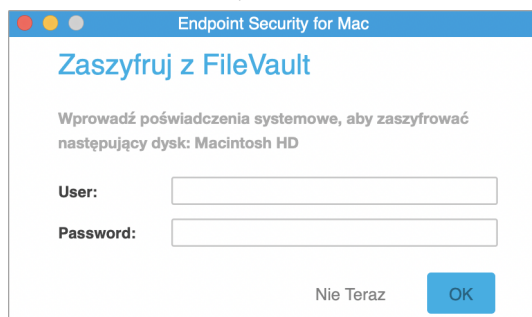
Acest capitol acoperă următoarele subiecte:

- [Criptarea volumelor](#)
- [Decriptarea volumelor](#)
- [Modificarea cheii de recuperare](#)
- [Modificarea parolei de criptare](#)

#### 3.1. Criptarea volumelor

Atunci când se aplică o politică de criptare pe Mac-ul dumneavoastră:

- Pentru unitățile de disc de tip boot:
  1. Vi se va solicita prin intermediul unei ferestre de dialog să introduceți numele de utilizator și parola pentru accesarea sistemului.



The screenshot shows a dialog box titled "Zaszyfruj z FileVault" from "Endpoint Security for Mac". The text inside reads: "Wprowadź poświadczenia systemowe, aby zaszyfrować następujący dysk: Macintosh HD". Below this, there are two input fields: "User:" and "Password:". At the bottom right, there is a blue "OK" button and the text "Nie Teraz" (Not Now).

2. Selectați butonul **OK** pentru inițierea procesului de criptare.

Dacă selectați opțiunea **Nu acum**, procesul de criptare este amânat, însă după o vreme se va afișa o fereastră de dialog, care va continua să apară cât timp politica de criptare este activă pe Mac.

3. După închiderea ferestrei **Criptare cu FileVault**, se întâmplă următorul lucru:
  - Dacă aveți un Mac care rulează o versiune de sistem de operare mai veche decât macOS Catalina (10.15), procesul de criptare începe imediat.
  - Dacă aveți un Mac care rulează macOS Catalina (10.15), Endpoint Security for Mac („fdesetup”) va solicita, printr-o fereastră suplimentară, aprobarea dvs. pentru activarea FileVault. Selectați butonul **OK** pentru a începe criptarea. Dacă selectați **Nu permite**, Endpoint Security for Mac nu va începe criptarea și va solicita aprobarea dvs. la fiecare câteva minute.



### Notă

În cazul sistemelor dual-boot, celălalt volum de tip boot nu va fi criptat.

- Pentru unitățile de disc de tip non-boot:
  1. Se va afișa o fereastră de dialog prin care vi se va solicita să configurați o parolă dedicată pentru criptarea fiecărei unități de disc. Această parolă este necesară numai pentru a debloca o anumită unitate de disc de tip non-boot.
  2. Selectați **Salvare**. Procesul de criptare va începe imediat.

Dacă selectați opțiunea **Anulare**, procesul de criptare este amânat. După o vreme, se va afișa o fereastră de dialog, iar aceasta va continua să apară cât timp politica de criptare este activă pe Mac.

Endpoint Security for Mac

## Ustaw hasło szyfrowania

NonBoot

Wybierz hasło

Potwierdź hasło

---

Wymagania hasła:

- ✘ Ma od 8 do 30 znaków
- ✘ Powinno zawierać wielkie i małe litery
- ✘ Powinno zawierać liczbę

Dismiss

Dacă Mac-ul are mai multe unități de disc, se vor afișa simultan ferestrele de dialog pentru criptare aferente tuturor unităților de disc.

## 3.2. Decriptarea volumelor

Atunci când se aplică o politică de decriptare pe Mac-ul dumneavoastră:

- Pentru unitățile de disc de tip boot:
  1. Vi se va solicita prin intermediul unei ferestre de dialog să introduceți numele de utilizator și parola pentru accesarea sistemului.
  2. Selectați **OK**. Procesul de decriptare va începe imediat.
- Pentru unitățile de disc de tip non-boot:
  1. Vi se va solicita prin intermediul unei ferestre de dialog să introduceți parola de criptare.
  2. Selectați **Salvare**. Procesul de decriptare va începe imediat.

Dacă selectați opțiunea **Anulare**, procesul de decriptare este amânat. După o vreme, se va afișa o fereastră de dialog, iar aceasta va continua să apară cât timp politica de criptare este activă pe Mac.



Dacă Mac-ul are mai multe unități de disc, se vor afișa simultan ferestrele de dialog pentru decriptare aferente tuturor unităților de disc.

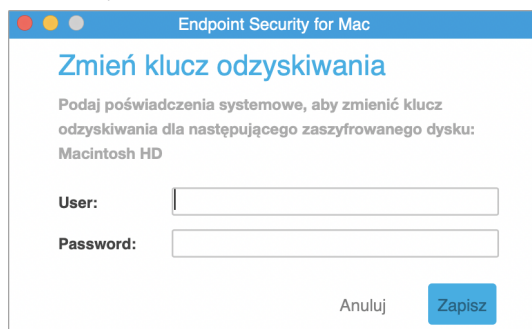
### 3.3. Modificarea cheii de recuperare

După începerea procesului de criptare, Endpoint Security for Mac trimite o cheie de recuperare către consola de administrare a administratorului de securitate. Cheia de recuperare este utilă pentru administratorul de securitate în cazul în care ați uitat datele de conectare sau parolele de criptare și nu puteți debloca unitățile de disc sau în cazul în care pe Mac există un alt utilizator care nu poate accesa una dintre unitățile de disc.

Puteți modifica cheia de recuperare pentru unitatea de disc de tip boot fără a fi nevoie să modificați datele de conectare.

Pentru a modifica cheia de recuperare pentru criptare aferentă unității de disc de tip boot:

1. Din fereastra principală a Endpoint Security for Mac, selectați unitatea de disc de tip boot criptată.
2. Selectați opțiunea **Modificare cheie de recuperare**.
3. Introduceți numele dvs. de utilizator și parola pentru accesarea sistemului.
4. Faceți clic pe butonul **Salvează**.



Endpoint Security for Mac

### Zmień klucz odzyskiwania

Podaj poświadczenia systemowe, aby zmienić klucz odzyskiwania dla następującego zaszyfrowanego dysku:  
Macintosh HD

User:

Password:

Anuluj

Opțiunea de a modifica cheia de recuperare este disponibilă numai dacă pe Mac-ul dumneavoastră este aplicată o politică de criptare.

În cazul în care modificați parola de sistem, unitatea de disc de tip boot criptată va rămâne neschimbată, fără a fi necesară intervenția dumneavoastră.

## 3.4. Modificarea parolei de criptare

Puteți schimba parola de criptare pentru unitățile de disc de tip non-boot din interfața de utilizator Endpoint Security for Mac. După schimbarea parolei, Endpoint Security for Mac va trimite o nouă cheie de recuperare către consola de administrare a administratorului de securitate.

Pentru a modifica parola de criptare pentru o unitate de disc de tip non-boot:

1. Din fereastra principală a Endpoint Security for Mac, selectați denumirea unității de disc criptate.
2. Selectați opțiunea **Modificare parolă**.
3. În fereastra **Modificare parolă de criptare**, configurați noua parolă.
4. Selectați opțiunea **Salvare**.

Endpoint Security for Mac

### Zmień hasło szyfrowania

NonBoot

Stare hasło

Wybierz hasło

Potwierdź hasło

Wymagania hasła:

- ✘ Ma od 8 do 30 znaków
- ✘ Powinno zawierać wielkie i małe litery
- ✘ Powinno zawierać liczbę

Dismiss

Opțiunea de a modifica parola de criptare este disponibilă numai dacă pe Mac-ul dumneavoastră este aplicată o politică de criptare.

## 4. CONFIGURAREA PREFERINȚELOR

Endpoint Security for Mac oferă un set minim de opțiuni ce pot fi configurate de către utilizator, deoarece soluția este administrată de administratorul de rețea prin intermediul politicii de securitate.

Acest capitol acoperă următoarele subiecte:

- [Accesarea preferințelor](#)
- [Carantină](#)
- [Istoric](#)
- [Preferințe de scanare](#)

### 4.1. Accesarea preferințelor

Pentru a deschide fereastra **Preferințe**:

1. Deschide Endpoint Security for Mac
2. Puteți proceda în oricare dintre următoarele modalități:
  - Faceți clic pe Endpoint Security for Mac din meniul Aplicații și selectați **Preferințe**.
  - Faceți clic dreapta pe pictograma Bitdefender din meniul Stare și selectați **Preferințe**.
  - Apăsăți tastele comandă-virgulă (,).
3. Faceți clic pe fila corespunzătoare caracteristicii pe care doriți să o configurați. Acestea sunt descrise în continuare.

### 4.2. Carantină

Secțiunea Carantină afișează toate fișierele izolate în directorul Carantină de pe calculatorul dumneavoastră local.

Pentru a șterge un fișier din carantină, selectați-l și faceți clic pe **Ștergere**. Dacă doriți să restaurați un fișier din carantină înapoi în locația sa inițială, selectați-l și faceți clic pe **Restaurează**.

### 4.3. Istoric

Endpoint Security for Mac menține un jurnal detaliat al evenimentelor legate de activitatea sa pe calculatorul dumneavoastră. Oricând intervine ceva relevant

pentru securitatea sistemului sau datelor dumneavoastră, se adaugă un mesaj nou în Istoricul Endpoint Security for Mac. Evenimentele reprezintă un instrument foarte important pentru monitorizarea și administrarea protecției calculatorului dumneavoastră. De exemplu, puteți verifica cu ușurință dacă actualizarea a fost finalizată cu succes, dacă a fost identificat vreun program malware pe calculatorul dumneavoastră etc.

Oricând doriți să ștergeți istoricul, faceți clic pe butonul **Ștergere istoric**. Butonul **Copiere** vă oferă posibilitatea să copiați aceste informații în clipboard.

## 4.4. Preferințe de scanare

Această fereastră vă permite să alegeți dacă doriți ca Endpoint Security for Mac să scaneze inclusiv fișierele de backup. Aplicația vă va informa doar dacă există o amenințare, întrucât OS X protejează discul Time Machine și împiedică ștergerea de fișiere de către Endpoint Security for Mac. Dacă se întâmplă ca aceasta să restaureze ulterior fișiere infectate, Endpoint Security for Mac le va detecta automat și va lua măsurile corespunzătoare.

În mod implicit, fișierele de backup sunt excluse de la scanare. Debifați caseta **Nu scana discul Time Machine** pentru a scana inclusiv această locație.

## 5. FOLOSIND INSTRUMENTUL LINIE DE COMANDĂ

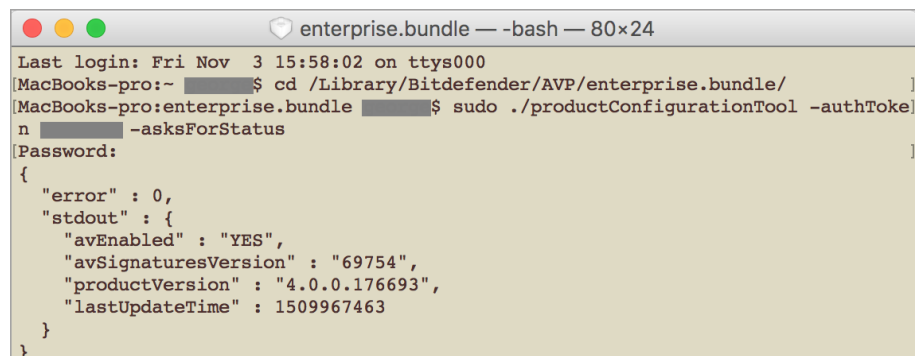
Soluția de securitate pentru stațiile de lucru pentru Mac vă permite să efectuați anumite sarcini folosind un instrument de linie de comandă numit **productConfigurationTool**. Mai precis, puteți obține informații despre starea produsului și puteți efectua scanări rapide și complete.

Pentru a folosi **productConfigurationTool**:

1. Deschideți **Terminal** pe computerul dumneavoastră.
2. Schimbați directorul de lucru folosind următoarea comandă:

```
cd /Library/Bitdefender/AVP/enterprise.bundle/
```

3. Rulați comenzile suportate cu privilegiile de administrator (comanda sudo).



```
enterprise.bundle — -bash — 80x24
Last login: Fri Nov  3 15:58:02 on ttys000
MacBooks-pro:~ ██████$ cd /Library/Bitdefender/AVP/enterprise.bundle/
MacBooks-pro:enterprise.bundle ██████$ sudo ./productConfigurationTool -authToken ██████ -asksForStatus
Password:
{
  "error" : 0,
  "stdout" : {
    "avEnabled" : "YES",
    "avSignaturesVersion" : "69754",
    "productVersion" : "4.0.0.176693",
    "lastUpdateTime" : 1509967463
  }
}
```

Folosirea **productConfigurationTool** din Terminal

Acest capitol cuprinde următoarele subiecte legate de **productConfigurationTool**:

- [Comenzi acceptate](#)
- [Parametrul codului de autentificare](#)
- [Coduri de eroare](#)

### 5.1. Comenzi acceptate

Interfața **productConfigurationTool** suportă următoarele comenzi:

## solicităstare

Extrage informații despre:

- Starea modulului anti-malware (activat sau dezactivat).
- Versiunea semnăturilor anti-malware.
- Versiune produs.
- Data efectuării ultimei actualizări.

Cum se folosește:

```
sudo ./productConfigurationTool -authToken [password]
-asksForStatus
```

Exemplu de output în caz de succes:

```
{
  "error" : 0,
  "stdout" : {
    "avEnabled" : "YES",
    "avSignaturesVersion" : "69440",
    "productVersion" : "4.0.0.175873",
    "lastUpdateTime" : 1507185205
  }
}
```

Exemplu de output în caz de eșec:

```
"error" : 100
```

## solicităefectuarescanare

Pornește o sarcină de scanare, furnizând la final detalii despre proces: total articole scanate, durată scanare, cale registru și dacă au survenit sau nu infecții.

Această comandă este urmată de un identificator predefinit pentru fiecare tip de sarcină de scanare:

- **Scanare rapidă** (ID: da29f7c8-23b1-4974-8d11-209959ac694b) – această sarcină este configurată pentru un nivel de bază de securitate și

utilizare redusă a resurselor. Principalele ținte de scanare sunt procesele aflate în curs și unele locații vulnerabile. Doar o singură instanță a acestei sarcini poate rula la un moment dat.

Cum se realizează o scanare rapidă:

```
sudo ./productConfigurationTool -authToken  
[password] -asksForAScanToRun  
da29f7c8-23b1-4974-8d11-209959ac694b
```

- **Scanare completă** (ID: dcf483c4-26d0-4e6f-ba28-6a53a00adae1) – această sarcină este configurată la un nivel maxim de protecție contra oricărui tip de malware. Numai o singură instanță poate fi rulată la un moment dat.

Cum se realizează o scanare completă:

```
sudo ./productConfigurationTool -authToken  
[password] -asksForAScanToRun  
dcf483c4-26d0-4e6f-ba28-6a53a00adae1
```

Exemplu de output în caz de succes după executarea comenzii solicităefectuarescanare

```
{  
  "error" : 0,  
  "stdout" : {  
    "scanDuration" : 13,  
    "logfilepath" : "\\Library\\Application Support\  
    /Antivirus for Mac\\Logs\  
    /da29f7c8-23b1-4974-8d11-209959ac694b.xml",  
    "totalScanned" : 6158,  
    "infection" : "NO"  
  }  
}
```

Exemplu de output în caz de eșec:

```
"error" : 95
```



### Notă

- Nu puteți efectua o scanare personalizată folosind **productConfigurationTool**.
- Unele sarcini de scanare pot dura mult până la finalizare. Spre exemplu, o scanare completă poate dura peste 20 de minute.

## 5.2. Parametrul codului de autentificare

Acest parametru vă ajută să preveniți utilizarea neautorizată a **productConfigurationTool**. Acesta trebuie inclus de fiecare dată când executați o comandă.



### Notă

Ca măsură temporară, parametrul `authToken` solicită o parolă pe care o puteți obține contactând echipa de asistență a Bitdefender.

## 5.3. Coduri de eroare

Interfața **productConfigurationTool** poate prezenta unul dintre următoarele coduri de eroare:

Eroare	Descriere
100	Parametrii <b>productConfigurationTool</b> nu sunt <b>corecți</b> .
99	Instrumentul nu funcționează cu drepturi de administrator.
98	<code>"/Library/Bitdefender/AVP/enterprise.bundle/epsdk.dylib"</code> nu a fost găsit. Actualizați produsul.
97	Încărcarea funcțiilor de tip <code>f_EPSDK_GetInstance</code> și <code>f_EPSDK_ReleaseInstance</code> din bibliotecă a eșuat. Actualizați produsul.
96	Răspunsul <code>.json</code> nu are anumite câmpuri preconizate sau are un format diferit decât cel preconizat. Actualizați produsul.
95	O anumită interogare solicită evenimentelor să obțină toate datele relevante, însă nu toate evenimentele sunt interceptate. Actualizați produsul. Dacă eroarea persistă, contactați echipa de asistență Bitdefender.



Eroare	Descriere
94	"/Library/Bitdefender/AVP/EndpointSecurityforMac.app/Contents/Info.plist" nu a fost găsit sau "CFBundleVersion" nu a fost găsit în fișierul .plist. Actualizați produsul.
93	<b>productConfigurationTool</b> nu este suportat de această versiune a soluției de securitate pentru stațiile de lucru pentru Mac. Actualizați produsul.
92	Parola authToken furnizată nu corespunde valorii preconizate.
0	Comanda a fost executată cu succes.

## 6. ÎNTREBĂRI FRECVENTE

**Jurnalul de scanare indică faptul că există încă o serie de obiecte nesoluționate. Cum le șterg?**

Obiectele nesoluționate din jurnalul de scanare pot fi:

- acces restricționat arhive (xar, rar, etc.)

**Soluție:** Utilizați opțiunea **Arată în Finder** pentru a identifica fișierul și pentru a-l șterge manual. Goliți folderul Trash.

- acces restricționat cutii poștale (Thunderbird, etc.)

**Soluție:** Utilizați aplicația pentru a șterge înregistrarea care conține fișierul infectat.

- fișiere ale altui utilizator

**Soluție:** Utilizați opțiunea **Arată în Finder** pentru a identifica fișierul și contactați proprietarul acestuia pentru a afla dacă se poate șterge în siguranță fișierul respectiv. În cazul în care se poate șterge în siguranță fișierul respectiv, ștergeți-l manual. Goliți folderul Trash.



### Notă

Fișiere cu acces restricționat înseamnă fișiere pe care Endpoint Security pentru Mac le poate doar deschide, dar nu le poate modifica.



### Pot actualiza Endpoint Security pentru Mac printr-un server proxy?

Endpoint Security pentru Mac se poate actualiza numai prin servere proxy care nu necesită autentificare. Nu trebuie să configurați nicio setare de program.

Dacă vă conectați la internet prin intermediul unui server proxy ce necesită autentificare, trebuie să treceți în mod regulat la o conexiune directă la internet pentru a putea obține actualizările semnăturilor softurilor periculoase.

### Cum șterg extensiile TrafficLight din browser-ul meu web?

- Pentru a șterge extensiile TrafficLight din Mozilla Firefox, urmați pașii de mai jos:
  1. Deschideți browser-ul Mozilla Firefox.
  2. Mergeți la **Instrumente** și selectați **Add-ons**.
  3. Selectați **Extensii** din coloana din partea stângă.

4. Selectați extensia și faceți clic pe **Ștergere**.
  5. Reporniți browser-ul pentru finalizarea procesului de ștergere.
- Pentru a șterge extensiile TrafficLight din Google Chrome, urmați pașii de mai jos:
    1. Deschideți browser-ul Google Chrome.
    2. Faceți clic pe  din toolbar-ul browser-ului.
    3. Mergeți la **Instrumente** și selectați **Extensii**.
    4. Selectați extensia și faceți clic pe **Ștergere**.
    5. Faceți clic pe **Dezinstalare** pentru a confirma procesul de ștergere.
  - Pentru a elimina Bitdefender TrafficLight din Safari, urmați pașii de mai jos:
    1. Deschideți browser-ul Safari.
    2. Faceți clic pe  din bara de instrumente a browserului și faceți clic pe **Preferences**.
    3. Selectați tabul **Extensions** și identificați extensia **Bitdefender TrafficLight on Safari** în listă.
    4. Selectați extensia și faceți clic pe **Dezinstalare**.
    5. Faceți clic pe **Dezinstalare** pentru a confirma procesul de ștergere.

## 7. OBȚINERE AJUTOR

Pentru orice probleme sau întrebări referitoare la Endpoint Security pentru Mac, vă rugăm să contactați administratorul de rețea.

Deschideți fereastra **About Endpoint Security for Mac** pentru a găsi produsul și informațiile de contact:

1. Deschide Endpoint Security for Mac
2. Faceți click pe **Endpoint Security for Mac** în bara de meniu.
3. Alege **Despre Endpoint Security for Mac**.

## Tipuri de softuri periculoase

### adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

### Keylogger

Un keylogger este o aplicație care înregistrează orice tasteți.

Înregistratoarele de taste au o natură periculoasă. Acestea pot fi utilizate în scopuri legitime, ca de exemplu pentru monitorizarea activității copiilor sau angajaților. Totuși, sunt folosite din ce în ce mai mult de infractorii cibernetici în scopuri negative (ca de exemplu, pentru a colecta date personale, cum ar fi acreditările de înregistrare și codurile numerice personale).

### Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la unelte recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

## Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei permise ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

## Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai insidioase tipuri de troieni este acela care pretinde că elimină virușii de pe calculatorul dumneavoastră, dar în loc de aceasta introduce viruși pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

## Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.

## Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

## Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu are un tipar binar consistent, asemenea viruși sunt greu de identificat.