



Bitdefender®

GravityZone



GHID DE INSTALARE

Bitdefender GravityZone Ghid de Instalare

Publicat 2021.01.13

Copyright© 2021 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 ținuti responsabili față de nici o 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 linkuri către siteuri web aparținând unor terți, care nu se află sub controlul Bitdefender; prin urmare, Bitdefendernu este responsabilă pentru conținutul respectivelor siteuri. Responsabilitatea accesării oricăruia dintre siteurile terților al căror link este furnizat în acest document vă aparține în totalitate. Bitdefender furnizează aceste linkuri 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

Prefață	vi
1. Convenții utilizate în ghid	vi
1. Despre GravityZone	1
2. Stratouri de protecție GravityZone	2
2.1. Antimalware	2
2.2. Advanced Threat Control	3
2.3. HyperDetect	4
2.4. Anti-Exploit avansat	4
2.5. Firewall	4
2.6. Content Control	5
2.7. Network Attack Defense	5
2.8. Administrarea patch-urilor	5
2.9. Device Control	5
2.10. Full Disk Encryption	6
2.11. Security for Exchange	6
2.12. Sandbox Analyzer	6
2.13. Soluție EDR (Endpoint Detection and Response)	7
2.14. Endpoint Risk Analytics (ERA)	8
2.15. Email Security	8
2.16. Disponibilitatea straturilor de protecție GravityZone	8
3. Arhitectura GravityZone	9
3.1. Consola web (GravityZone Control Center)	9
3.2. Security Server	9
3.3. Agenți de securitate	9
3.3.1. Bitdefender Endpoint Security Tools	9
3.3.2. Endpoint Security for Mac	12
3.4. Arhitectura Sandbox Analyzer	12
3.5. Arhitectura EDR	14
4. Cerințe	16
4.1. Control Center	16
4.2. Protecția pentru endpoint-uri	16
4.2.1. Hardware	17
4.2.2. Sisteme de operare suportate	20
4.2.3. Sisteme de fișiere acceptate	26
4.2.4. Browsere compatibile	26
4.2.5. Security Server	27
4.2.6. Utilizarea pentru trafic	28
4.3. Protecție Exchange	30
4.3.1. Medii compatibile Microsoft Exchange	30
4.3.2. Cerințe de sistem	31
4.3.3. Alte cerințe software	31
4.4. Full Disk Encryption	31
4.5. Porturile de comunicare GravityZone	33

5. Instalarea protecției	34
5.1. Administrarea licenței	34
5.1.1. Găsirea unui distribuitor	34
5.1.2. Activarea licenței	34
5.1.3. Verificare detalii licență curentă în curs	35
5.2. Instalarea Endpoint Protection	35
5.2.1. Instalarea Security Server	36
5.2.2. Instalarea agenților de securitate	39
5.3. Instalarea EDR	63
5.4. Instalarea Full Disk Encryption	64
5.5. Instalarea Exchange Protection	65
5.5.1. Pregătirea pentru instalare	65
5.5.2. Instalarea protecției pe serverele Exchange	66
5.6. Manager Credențiale	66
5.6.1. Adăugare de date în modulul Administrare Date de Autentificare	67
5.6.2. Ștergerea datelor din fereastra Administrare Date de Autentificare	68
6. Integrări	69
6.1. Integrare cu ConnectWise Automate	69
6.2. Integrare cu ConnectWise Manage	69
6.3. Integrarea cu Amazon EC2	70
6.4. Integrarea cu Splunk	70
6.5. Integrare cu Kaseya VSA	70
6.6. Integrare cu Datto RMM	70
7. Dezinstalarea protecției	71
7.1. Dezinstalarea Endpoint Protection	71
7.1.1. Dezinstalarea agenților de securitate	71
7.1.2. Dezinstalarea Security Server	73
7.2. Dezinstalarea Exchange Protection	73
8. Obținere ajutor	75
8.1. Centrul de asistență Bitdefender	75
8.2. Solicitarea de asistență profesională	76
8.3. Utilizarea Modulului de Suport Tehnic	76
8.3.1. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Windows	77
8.3.2. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Linux	78
8.3.3. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Mac	80
8.4. Informații de contact	81
8.4.1. Adrese Web	81
8.4.2. Distribuitori locali	81
8.4.3. Filialele Bitdefender	82
A. Anexe	85
A.1. Tipuri de fișiere acceptate	85
A.2. Obiecte Sandbox Analyzer	86
A.2.1. Tipuri și extensii de fișiere acceptate pentru trimitere manuală	86
A.2.2. Tipurile de fișiere acceptate de modulul de filtrare preliminară a conținutului la trimiterea automată	86



A.2.3. Excluderi implicite la trimiterea automată	87
A.3. Kerneluri compatibile cu senzorul de incidente	87

Prefață

Acest ghid este destinat companiilor Partenerie Bitdefender, care oferă GravityZone ca serviciu de securitate clienților lor. Ghidul este destinat administratorilor IT care se ocupă de securitatea rețelei companiei lor și rețelele clienților lor.

Acest document are ca scop să explice modul de instalare a agenților de securitate Bitdefender pe toate tipurile de stații de lucru în cadrul companiilor administrate și modul de configurare a soluției GravityZone.

1. Convenții utilizate în ghid




Convenții tipografice

Acest ghid folosește mai multe stiluri de text pentru o lizibilitate îmbunătățită. Aflați mai multe despre aspectul și însemnătatea acestora din tabelul de mai jos.

Aspect	Descriere
mostră	Numele de comenzi inline, sintaxele, căile și numele de fișiere, output-urile fișierelor de configurare și textele de intrare sunt tipărite cu caractere de tip monospațiat.
http://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
gravityzone-docs@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.
„Prefață” (p. vi)	Acesta este un link intern, către o locație din document.
opțiuni	Toate opțiunile produsului sunt tipărite cu caractere bold .
cuvânt cheie	Opțiunile de interfață, cuvintele cheie sau scurtăturile sunt evidențiate cu ajutorul caracterelor aldine .

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 sunt furnizate informații importante, dar care nu sunt critice.
-  **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 este descris ceva extrem de riscant.

1. DESPRE GRAVITYZONE

GravityZone este un produs prevăzut cu o consolă de administrare unică, disponibilă în cloud, găzduită de Bitdefender, sau ca aplicație virtuală ce se instalează la sediul companiei și asigură un punct unic pentru configurarea, aplicarea și administrarea politicilor de securitate pentru un număr nelimitat de stații de lucru de orice tip, indiferent de locul în care se află.

GravityZone oferă mai multe niveluri de securitate pentru stațiile de lucru și pentru serverele de e-mail Microsoft Exchange: antimalware cu monitorizarea comportamentului, protecția contra amenințărilor în ziua zero, lista neagră de aplicații și sandboxing, firewall, controlul dispozitivelor, controlul conținutului, anti-phishing și antispam.

2. STRATURI DE PROTECȚIE GRAVITYZONE

GravityZone oferă următoarele straturi de protecție:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Anti-Exploit avansat
- Firewall
- Content Control
- Administrarea patch-urilor
- Device Control
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Soluție EDR (Endpoint Detection and Response)
- Endpoint Risk Analytics (ERA)
- Email Security

2.1. Antimalware

Nivelul de protecție antimalware se bazează pe scanarea semnăturilor și analiza euristică (B-HAVE, ATC) împotriva: virușilor, troienilor, atacurilor de tip worm, spyware, adware, keylogger, rootkit și alte tipuri de software periculos

Tehnologia de scanare antimalware a Bitdefender se bazează pe următoarele tehnologii:

- În primul rând, se folosește o metodă de scanare tradițională acolo unde conținutul se potrivește cu baza de date de semnături. Baza de date de semnături conține modele de bytes specifice amenințărilor cunoscute și este actualizată în mod regulat de Bitdefender. Această metodă de scanare este eficientă împotriva amenințărilor confirmate care au fost cercetate și documentate. Cu toate acestea, indiferent cât de prompt este actualizată baza de date, există întotdeauna o fereastră de vulnerabilitate între momentul când se descoperă o nouă amenințare și momentul lansării unei remedieri..
- Împotriva amenințărilor noi și nedocumentate, se asigură un al doilea strat de protecție de către **B-HAVE**, motorul euristic al Bitdefender. Algoritmii euristici detectează programele malware pe baza caracteristicilor comportamentale. B-HAVE execută fișierele suspecte într-un mediu virtual pentru a testa impactul

acestora asupra sistemului și pentru a se asigura că nu prezintă o amenințare. Dacă se detectează o amenințare, se blochează executarea programului.

Motoare de scanare

Bitdefender GravityZone poate configura automat motoarele de scanare la crearea pachetelor de agenți de securitate, în funcție de configurația endpointului.

Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:

1. **Scanare locală**, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având conținutul de securitate stocat local.
2. **Scanarea hibrid cu motoare light (Cloud public)**, cu o amprentă medie, folosind scanarea în cloud și, parțial, conținut de securitate. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
3. **Scanarea centralizată în cloud-ul public sau privat**, cu o amprentă redusă care necesită un Security Server pentru scanare. În acest caz, nu se stochează local niciun conținut de securitate, iar scanarea este transferată către Security Server.



Notă

Există un set minim de motoare stocate local, care sunt necesare pentru despachetarea fișierelor arhivate.

4. **Scanare centralizată (cloud public sau privat cu Security Server) cu fallback* pe Scanare locală (motoare full)**
5. **Scanare centralizată (Scanare în cloud public sau privat cu Security Server) cu fallback* pe Scanare hibrid (cloud public cu motoare light)**

* Atunci când se folosește scanarea cu motoare duble, dacă primul motor este indisponibil, se va folosi motorul de rezervă (fallback). Consumul de resurse și gradul de utilizare a rețelei vor depinde de motoarele folosite.

2.2. Advanced Threat Control

Pentru amenințări care scapă chiar și de motorul euristic, este prezent un alt strat de protecție sub forma unei funcții Advanced Threat Control (ATC).

Advanced Threat Control monitorizează în mod continuu procesele în curs și cataloghează comportamentele suspecte, precum tentativele de: deghizare a tipului

de proces, executare de cod în spațiul altui proces (furtul de memorie a procesului pentru escaladarea drepturilor), reproducerea, eliminarea fișierelor, ascunderea de aplicațiile de enumerare a proceselor etc. Fiecare comportament suspect duce la creșterea punctajului acordat proceselor. Atunci când se atinge un prag, se declanșează alarma.

2.3. HyperDetect

Bitdefender HyperDetect este un strat suplimentar de securitate conceput special pentru a detecta atacurile avansate și activitățile suspecte în faza de pre-execuție. HyperDetect conține modele de învățare automată (machine learning) și tehnologii de detectare a atacurilor ascunse pentru combaterea amenințărilor precum: atacuri de tip „zero-day”, amenințări persistente avansate (APT), malware ascuns, atacuri fără fișiere (utilizarea necorespunzătoare a PowerShell, Windows Management Instrumentation etc.), furtul de date de autentificare, atacuri targetate, malware personalizat, atacuri bazate pe scripturi, exploit-uri, instrumente de hacking, trafic suspect în rețea, aplicații potențial nedorite (PUA), ransomware.

Notă

Acest modul este un add-on disponibil în baza unui cod de licență separat.

2.4. Anti-Exploit avansat

Având la bază tehnologia de învățare automată (machine learning), tehnologia proactivă de Anti-Exploit Avansat oprește atacurile de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive. Modulul Anti-exploit avansat depistează în timp real cele mai recente exploit-uri și diminuează vulnerabilitățile de corupere a memoriei care pot trece nedetectate de către alte soluții de securitate. Protejează aplicațiile utilizate cel mai frecvent, cum ar fi browser-ele, Microsoft Office sau Adobe Reader, precum și alte aplicații la care vă puteți gândi. Veghează asupra proceselor de sistem și protejează împotriva breșelor de securitate și a furturilor din procesele existente.

2.5. Firewall

Firewall-ul controlează accesul aplicațiilor la rețea și internet. Accesul este permis automat pentru o bază de date cuprinzătoare de aplicații cunoscute și sigure. În plus, firewall-ul poate proteja sistemul împotriva scanărilor de porturi, poate restricționa ICS și poate emite avertizări atunci când la o conexiune Wi-Fi se adaugă noi noduri.

2.6. Content Control

Modulul de control al conținutului susține aplicarea politicilor companiei privind traficul permis, accesul la internet, protecția datelor și controlul aplicațiilor. Administratorii pot defini opțiunile de scanare a traficului și excepțiile, pot stabili un program pentru accesul la internet, blocând anumite categorii web sau URL-uri, pot configura regulile de protecție a datelor și pot defini drepturile pentru utilizarea anumitor aplicații.

2.7. Network Attack Defense

Modulul de protecție Network Attack Defense se bazează pe o tehnologie Bitdefender ce vizează detectarea atacurilor din rețea concepute pentru a obține acces la endpoint-uri folosind tehnici specifice, cum ar fi: atacuri de tip „brute force”, exploit-uri la nivel de rețea, furt de parole, vectori de infectare drive-by-download, bot-uri și troieni.

2.8. Administrarea patch-urilor

Complet integrat în GravityZone, Patch Management menține actualizate sistemele de operare și aplicațiile software și oferă o imagine completă asupra stării de aplicare a patch-urilor pe stațiile de lucru administrate, cu sistem de operare Windows.

Modulul GravityZone Patch Management include mai multe funcții, cum ar fi scanarea la cerere / programată a patch-urilor, instalarea automată / manuală a patch-urilor sau raportarea patch-urilor absente.

Puteți afla mai multe despre distribuitorii autorizați și produsele compatibile cu GravityZone Patch Management din acest [articol KB](#).



Notă

Patch Management este un add-on disponibil cu cheie de licență separată pentru toate pachetele GravityZone.

2.9. Device Control

Modulul Control dispozitiv împiedică scurgerile de date confidențiale și infecțiile cu malware folosind dispozitive externe atașate endpoint-ului, prin aplicarea unor reguli și excepții de blocare prin intermediul politicilor, pentru o gamă largă de tipuri

de dispozitive (cum ar fi unități de stocare flash USB, dispozitive Bluetooth, CD/DVD playere, dispozitive de stocare etc.).

2.10. Full Disk Encryption

Acest strat de protecție vă permite să asigurați caracteristica Full Disk Encryption pe endpoint-uri, gestionând funcția BitLocker pe Windows și funcțiile FileVault și diskutil pe macOS. Puteți cripta și decripta volume boot și non-boot, cu doar câteva clicuri, în timp ce GravityZone gestionează întregul proces, cu intervenție minimă din partea utilizatorilor. În plus, GravityZone stochează codurile de recuperare necesare pentru a debloca volumele atunci când utilizatorii își uită parolele.



Notă

Full Disk Encryption este un add-on disponibil cu o cheie de licență separată pentru toate pachetele GravityZone disponibile.

2.11. Security for Exchange

Bitdefender Security for Exchange asigură protecție antimalware, antispam, antiphishing, filtrare a conținutului și a fișierelor atașate, toate acestea complet integrate cu server-ul Microsoft Exchange, pentru a asigura un mediu securizat de comunicare prin mesaje și o productivitate sporită. Folosind tehnologiile antimalware și antispam premiate, aceasta protejează utilizatorii Exchange împotriva celor mai noi și mai sofisticate programe malware, precum și împotriva tentativelor de furt al datelor confidențiale sau valoroase ale utilizatorilor.



Important

Security for Exchange este proiectat pentru a proteja întreaga organizație Exchange de care aparține serverul Exchange protejat. Aceasta înseamnă că protejează toate căsuțele de e-mail active, inclusiv căsuțele de e-mail de tip user (utilizator) / room (cameră)/ equipment (echipament) / shared (partajat).



Notă

Acest modul este un add-on disponibil în baza unui cod de licență separat.

2.12. Sandbox Analyzer

Bitdefender Sandbox Analyzer oferă un nivel puternic de securitate împotriva amenințărilor avansate prin efectuarea unei analize automate și detaliate a fișierelor suspecte care nu sunt încă semnate de motoarele antimalware ale Bitdefender.

Sandbox-ul utilizează o serie de tehnologii Bitdefender pentru a executa sarcinile într-un mediu virtual închis, găzduit de Bitdefender, pentru a analiza comportamentul acestora și raporta orice schimbări subtile aduse sistemului, care semnaleză intenții periculoase.

Sandbox Analyzer trimite automat fișierele suspecte de pe stațiile de lucru administrate, care rămân ascunse de serviciile anti-malware pe bază de semnătură. Euristica dedicată integrată în modulul antimalware de scanare la accesare din cadrul Bitdefender Endpoint Security Tools declanșează acest proces de trimitere.

Serviciul Sandbox Analyzer este capabil să prevină executarea unor amenințări necunoscute pe stația de lucru. Acesta operează fie în modul de monitorizare, fie în modul de blocare, permițând sau blocând accesul fișierelor suspecte, până la primirea unui verdict. Sandbox Analyzer soluționează automat orice amenințări detectate, conform acțiunilor de remediere definite în politica de securitate pentru sistemele afectate.

În plus, Sandbox Analyzer vă permite să trimiteți manual mostre direct din Control Center, lăsându-vă pe dumneavoastră să decideți ce se va întâmpla în continuare cu ele.



Important

Încărcarea manuală este permisă utilizatorilor GravityZone cu drepturi de **Administrare rețele**.



Notă

Acest modul este un add-on disponibil în baza unui cod de licență separat.

2.13. Soluție EDR (Endpoint Detection and Response)

Detectarea și Răspunsul Stației de Lucru (EDR) este o componentă corelată cu evenimentele, capabilă să identifice amenințări avansate sau atacuri în curs de desfășurare. Ca parte a Platformei noastre cuprinzătoare și integrate de Protecție a Stațiilor de Lucru, EDR aduce inteligența dispozitivelor în rețeaua companiei dumneavoastră. Această soluție vine în ajutorul eforturilor echipelor dumneavoastră responsabile cu răspunsul la incidente pentru a investiga și a reacționa la amenințări avansate.

Prin intermediul Bitdefender Endpoint Security Tools, puteți activa un modul de protecție denumit EDR pe stațiile de lucru pe care le administrați, pentru a colecta date despre hardware și sistemul de operare. Respectând un cadru de lucru client-server, metadatele sunt colectate și procesate de ambele părți.

Această componentă aduce informații detaliate cu privire la incidentele detectate, o hartă interactivă a incidentelor, acțiuni de remediere și integrare cu Sandbox Analyzer și HyperDetect.

**Notă**

Acest modul este un add-on disponibil în baza unui cod de licență separat.

2.14. Endpoint Risk Analytics (ERA)

Endpoint Risk Analytics (ERA - Analiza riscurilor asupra stațiilor de lucru) identifică, evaluează și remediază slăbiciunile stațiilor de lucru Windows prin intermediul unor scanări ale riscurilor de securitate (la cerere sau programate în funcție de politică), luând în calcul un număr mare sau indicatori de risc. O dată ce ați scanat rețeaua cu anumiți indicatori de risc, veți obține o vedere de ansamblu asupra stării de risc a rețelei dvs. prin intermediul panoului **Administrarea riscului**, disponibil din meniul principal. Veți putea soluționa anumite riscuri de securitate automat din Control Center GravityZone, și veți putea vizualiza recomandările pentru diminuarea expunerii stațiilor de lucru.

2.15. Email Security

Cu ajutorul Email Security puteți controla livrarea e-mail-urilor, filtra mesajele și aplica politici la nivelul întregii companii, pentru a bloca amenințările targetate și sofisticate transmise prin e-mail, inclusiv atacurile de tip „BEC” (Business Email Compromise) și „CEO fraud”. Email Security necesită drepturi de acces la cont pentru a accesa consola. Pentru mai multe informații, consultați [Bitdefender Email Security Ghidul utilizatorului](#).

2.16. Disponibilitatea straturilor de protecție GravityZone

Disponibilitatea nivelurilor de protecție GravityZone diferă în funcție de sistemul de operare al stației de lucru. Pentru a afla mai multe, consultați articolul KB [Disponibilitatea nivelurilor de protecție GravityZone](#).

3. ARHITECTURA GRAVITYZONE

Soluția GravityZone include următoarele componente:

- [Consola web \(Control Center\)](#)
- [Security Server](#)
- [Agenți de securitate](#)

3.1. Consola web (GravityZone Control Center)

Control Center, o interfață pe platformă web, se integrează cu funcțiile existente de administrare a sistemului și cu sistemele de monitorizare pentru a facilita aplicarea protecției pe stații de lucru și serverele neadministrate.

3.2. Security Server

Security Server este o mașină virtuală dedicată, care anulează duplicatele și centralizează majoritatea funcționalităților antimalware ale agenților de securitate, acționând ca server de scanare.

Notă

Este posibil ca licența dumneavoastră să nu includă această caracteristică.

Security Server trebuie să fie instalat pe una sau mai multe gazde astfel încât să suporte numărul de mașini virtuale protejate.

3.3. Agenți de securitate

Pentru a proteja rețeaua cu Bitdefender, trebuie să instalați agenții de securitate GravityZone corespunzători pe stațiile de lucru din rețea.

- [Bitdefender Endpoint Security Tools](#)
- [Endpoint Security for Mac](#)

3.3.1. Bitdefender Endpoint Security Tools

GravityZone asigură protecția mașinilor Windows și Linux, fizice sau virtuale, cu Bitdefender Endpoint Security Tools, un agent de securitate inteligent, care ține cont de mediu și care se adaptează în funcție de tipul stației de lucru. Bitdefender Endpoint Security Tools poate fi instalat pe orice mașină, virtuală sau fizică,

asigurând un sistem de scanare flexibil, fiind alegerea ideală pentru mediile mixte (fizice, virtuale și în cloud).

Pe lângă protecția sistemului de fișiere, Bitdefender Endpoint Security Tools include și protecția serverului e-mail pentru Serverele Microsoft Exchange.

Bitdefender Endpoint Security Tools folosește un singur model de politică pentru mașinile fizice și virtuale, precum și o singură sursă pentru kit-ul de instalare pentru toate mediile (fizice ori virtuale) care rulează sistemul de operare Windows.

Straturi de protecție

Următoarele straturi de protecție sunt disponibile în cadrul Bitdefender Endpoint Security Tools:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Firewall
- Content Control
- Network Attack Defense
- Administrarea patch-urilor
- Device Control
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Soluție EDR (Endpoint Detection and Response)
- Endpoint Risk Analytics (ERA)

Roluri ale stațiilor de lucru

- Utilizator privilegiat
- Relay
- Server de cache pentru patch-uri
- Protecție Exchange

Utilizator privilegiat

Administratorii Control Center pot acorda drepturi de Utilizator privilegiat utilizatorilor de stații de lucru prin intermediul setărilor politicii de securitate. Modulul Utilizator privilegiat activează drepturile de administrare la nivel de utilizator, permițând utilizatorului stației de lucru să acceseze și să modifice setările

de securitate prin intermediul unei console locale. Control Center primește o notificare atunci când o stație de lucru este în modul Utilizator privilegiat, iar administratorul Control Center poate suprascrie oricând setările de securitate locale.



Important

Acest modul este disponibil numai pentru sistemele de operare pentru desktop și server Windows suportate. Pentru mai multe informații, consultă capitolul „Sisteme de operare suportate” (p. 20).

Relay

Agenții pentru stațiile de lucru cu rol de Bitdefender Endpoint Security Tools Relay sunt folosiți ca servere de comunicații proxy și actualizări pentru alte stații de lucru din rețea. Agenții pentru stațiile de lucru cu rol de relay sunt necesari în special pentru organizațiile cu rețele izolate, unde întregul trafic se desfășoară printr-un singur punct de acces.

În companiile cu rețele mari distribuite, agenții de tip relay ajută la scăderea gradului de utilizare a lățimii de bandă, prevenind conectarea stațiilor de lucru protejate și a serverelor de securitate direct la aplicația GravityZone.

După ce în rețea a fost instalat un agent Bitdefender Endpoint Security Tools Relay, celelalte stații de lucru pot fi configurate prin intermediul politicii pentru a comunica cu Control Center prin agentul de tip relay.

Agenții Bitdefender Endpoint Security Tools Relay sunt utilizați în următoarele scopuri:

- Descoperirea tuturor stațiilor de lucru neprotejate din rețea.
Această funcționalitate este esențială pentru instalarea agentului de securitate într-un mediu cloud GravityZone.
- Instalarea agentului pentru stații de lucru în rețeaua locală.
- Actualizarea stațiilor de lucru protejate din rețea.
- Asigurarea comunicării între Control Center și stațiile de lucru conectate.
- Acționarea ca server proxy pentru stațiile de lucru protejate.
- Optimizarea traficului în rețea în timpul actualizărilor, instalărilor, scanărilor și al altor sarcini consumatoare de resurse.

Server de cache pentru patch-uri

Stațiile de lucru cu rol de releu pot funcționa și ca server de cache pentru patch-uri. Având activat acest rol, releele sunt folosite pentru stocarea patch-urilor descărcate

de pe site-urile producătorilor de software și distribuirea lor pe stațiile de lucru din rețeaua dumneavoastră. De fiecare dată când o stație de lucru conține software cu patch-uri lipsă, acesta le ia de pe server și nu de pe site-ul producătorului, optimizând astfel traficul generat și gradul de ocupare a lățimii de bandă a rețelei.

Important

Acest rol suplimentar este disponibil cu un add-on Patch Management înregistrat.

Protecție Exchange

Bitdefender Endpoint Security Tools cu rolul de Exchange poate fi instalat pe serverele Microsoft Exchange cu scopul de a proteja utilizatorii Exchange de amenințările transmise prin e-mail.

Bitdefender Endpoint Security Tools cu rolul Exchange protejează atât serverul cât și soluția Microsoft Exchange.

3.3.2. Endpoint Security for Mac

Endpoint Security for Mac este un agent de securitate conceput pentru a proteja stațiile de lucru și laptopurile Macintosh cu tehnologie Intel. Tehnologia de scanare disponibilă este **Scanare localizată**, având conținut de securitate stocat local.

Straturi de protecție

Următoarele straturi de protecție sunt disponibile în cadrul Endpoint Security for Mac:

- [Antimalware](#)
- [Advanced Threat Control](#)
- [Content Control](#)
- [Device Control](#)
- [Full Disk Encryption](#)

3.4. Arhitectura Sandbox Analyzer

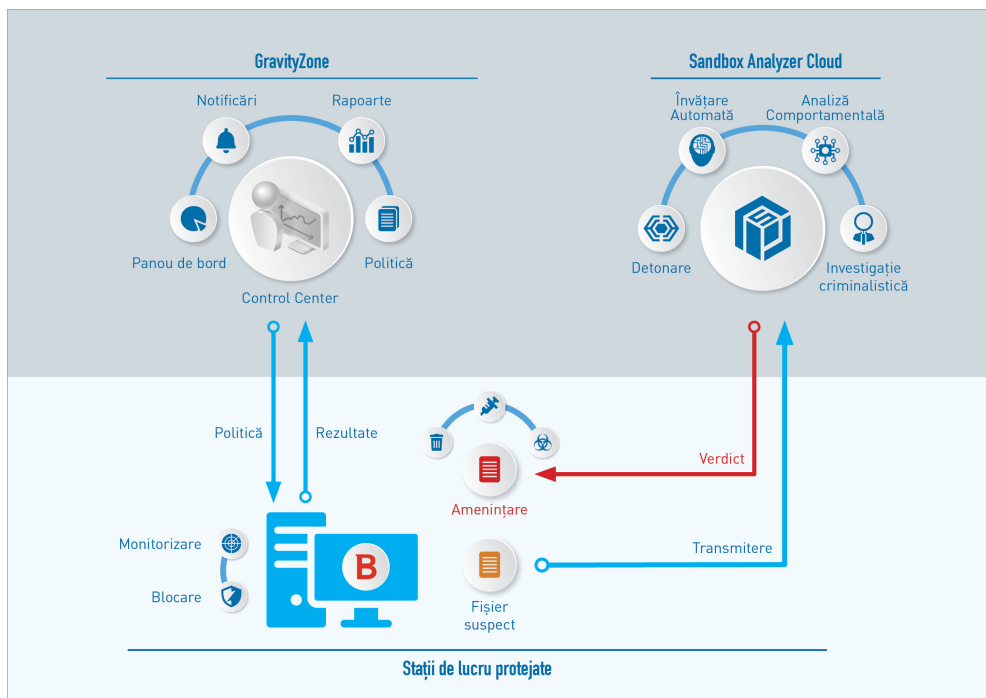
Bitdefender Sandbox Analyzer oferă un strat puternic de protecție împotriva amenințărilor avansate, efectuând analize automate în profunzime asupra fișierelor suspecte care nu sunt încă semnate de motoarele antimalware ale Bitdefender.

Sandbox Analyzer conține următoarele componente:

- **Portal Sandbox Analyzer.** Această componentă este un server de comunicații găzduit pentru gestionarea solicitărilor între endpoint-uri și cluster-ul sandbox al Bitdefender.
- **Cluster Sandbox Analyzer.** Această componentă constituie infrastructura sandbox găzduită în cadrul căreia are loc analiza comportamentală a mostrelor. La acest nivel, fișierele încărcate sunt detonate pe mașini virtuale cu sistem de operare Windows 7.

GravityZone Control Center operează ca o consolă de administrare și raportare, unde puteți configura politicile de securitate, vizualiza rapoarte și notificări.

Bitdefender Endpoint Security Tools, agentul de securitate instalat pe endpoint-uri, acționează ca senzor de alimentare pentru Sandbox Analyzer.



Arhitectura Sandbox Analyzer

Odată ce serviciul Sandbox Analyzer este activat din Control Center pe endpoint-uri:

1. Agentul de securitate Bitdefender începe să trimită fișiere suspecte care corespund regulilor de protecție definite în politica de securitate.
2. După ce fișierele sunt analizate, se trimite un răspuns înapoi către portal și apoi către stația de lucru.
3. Dacă un anumit fișier este detectat ca fiind periculos, utilizatorul primește o notificare și se întreprinde o măsură de remediere.

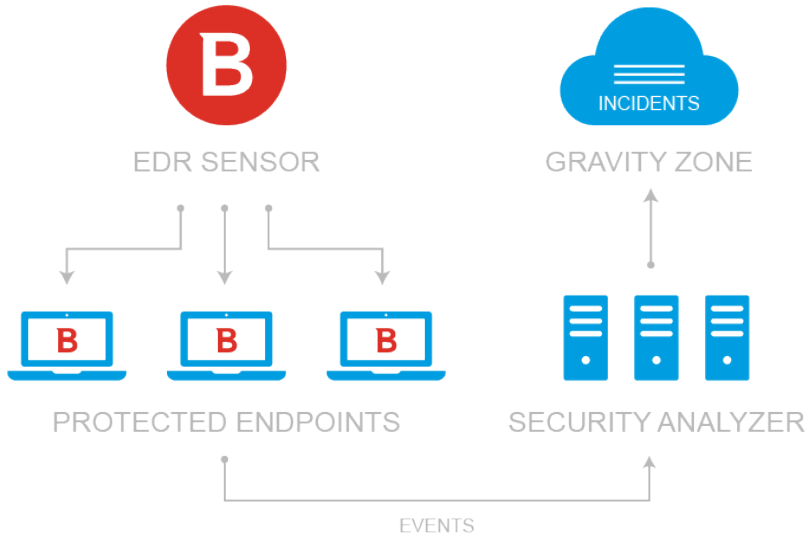
Rezultatele analizei sunt stocate în baza de date Sandbox Analyzer în funcție de valoarea hash a fișierului. Dacă un fișier analizat anterior este trimis din nou de la o stație de lucru diferită, se trimite imediat un răspuns înapoi întrucât rezultatele sunt deja disponibile în baza de date.

3.5. Arhitectura EDR

Pentru a identifica amenințările avansate și atacurile în curs de desfășurare, EDR are nevoie de date referitoare la hardware și sistemul de operare. Unele dintre datele brute sunt procesate la nivel local, în timp ce algoritmi automați de învățare din funcția Security Analytics execută sarcini de o complexitate mai ridicată.

EDR conține două componente majore:

- Senzorul de incidente, care colectează date despre procese și raportează datele comportamentale ale endpoint-urilor și aplicațiilor.
- Security Analytics, o parte componentă back-end a suitei de tehnologii Bitdefender utilizate pentru interpretarea metadatelor colectate de Senzorul de incidente.



Flux [EDR cu stații de lucru către Centrul de Comandă

4. CERINȚE

Toate soluțiile GravityZone sunt instalate și gestionate din Control Center.

4.1. Control Center

Pentru a accesa consola web Control Center, sunt necesare:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Rezoluție recomandată a ecranului: 1280 x 800 sau mai mare



Avertisment

Control Center nu va funcționa/nu se va afișa corespunzător în Internet Explorer 9+ cu funcția Compatibility View activată, care este echivalentă cu utilizarea unei versiuni de browser incompatibile.

4.2. Protecția pentru endpoint-uri

Pentru a proteja rețeaua cu Bitdefender, trebuie să instalați agenții de securitate GravityZone pe stațiile de lucru din rețea. În acest scop, aveți nevoie de un utilizator Control Center cu drepturi de administrator asupra serviciilor pe care trebuie să le instalați și asupra stațiilor de lucru din rețea pe care le administrați.

Cerințele pentru agentul de securitate sunt diferite, pornind de la existența rolurile existente pentru server, cum ar fi Releu, Protecția exchange sau Serverul de memorie cache pentru patch-uri. Pentru mai multe informații referitoare la rolurile agentului, consultați „Agenți de securitate” (p. 9).

4.2.1. Hardware

Agentul de securitate fără roluri

Uz procesor

Sistemele țintă	Tip CPU	Sisteme de operare (OS) compatibile
Stații de lucru	Procesoare compatibile cu Intel® Pentium, 2 GHz sau mai rapide	Sisteme de operare pentru desktop-urile care rulează Microsoft Windows.
	Intel® Core 2 Duo, 2 GHz sau mai rapid	macOS
Dispozitive inteligente	Procesoare compatibile cu Intel® Pentium, 800 MHz sau mai rapide	OS incluse în Microsoft Windows
Servere	Cerințe minime: Procesoare compatibile Intel® Pentium, 2,4 GHz	OS Microsoft Windows Server și OS Linux
	Recomandat: CPU Intel® Xeon multi-core, 1,86 GHz sau mai rapidă	



Avertisment

Procesoarele ARM nu sunt compatibile în prezent.

Memorie RAM disponibilă

La instalare (MB)

SO	MOTOR SIMPLU					
	Scanare locală		Scanare hibrid		Scanare central.	
	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	n/a	n/a	n/a	n/a

Pentru utilizare zilnică (MB)*



SO	Antivirus (motor simplu)			Module de protecție				
	Local	Hibrid	Centralizat	Scanare comportament	Firewall	Control conținut	Utilizator privilegiat	Server actualizări
Windows	75	55	30	+13	+17	+41	+29	+80
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

* Evaluările acoperă utilizarea zilnică a clientului stației de lucru, fără a lua în considerare sarcinile suplimentare, cum ar fi scanările la cerere sau actualizările de produs.

Eliberează spațiu de pe disc

La instalare (MB)

SO	MOTOR SIMPLU						MOTOR DUBLU			
	Scanare locală		Scanare hibrid		Scanare central.		Scanare central. + locală		Scanare central. + hibrid	
	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Pentru utilizare zilnică (MB)*

SO	Antivirus (motor simplu)			Module de protecție				
	Local	Hibrid	Centralizat	Scanare comportament	Firewall	Control conținut	Utilizator privilegiat	Server actualizări
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
macOS	1700	-	-	+20	-	+0	-	-

* Evaluările acoperă utilizarea zilnică a clientului stației de lucru, fără a lua în considerare sarcinile suplimentare, cum ar fi scanările la cerere sau actualizările de produs.

Agent de securitate cu rol de releu

Rolul de releu necesită resurse hardware suplimentare față de configurația de bază a agentului de securitate. Aceste cerințe trebuie să fie compatibile cu Serverul de actualizări și cu pachetele de instalare găzduite pe stația de lucru:

Număr de stații de lucru conectate	CPU compatibilă cu Serverul de actualizări	RAM	Spațiu liber pe hard disk pentru Serverul de actualizări
1-300	minim procesor Intel® Core™ i3 sau echivalent, 2 vCPU per nucleu	1.0 GB	10 GB
300-1000	minim procesor Intel® Core™ i5 sau echivalent, 4 vCPU per nucleu	1.0 GB	10 GB

Avertisment

- Procesoarele ARM nu sunt compatibile în prezent.
- Agenții de releu necesită discuri SSD, pentru a face față volumelor mari de operațiuni de citire/scriere.

Important

- Dacă doriți să salvați pachetele de instalare și actualizările pe o altă partiție decât cea pe care este instalat agentul, asigurați-vă că partițiile au spațiu liber suficient

pe hard disk (10 GB); în caz contrar, agentul va întrerupe instalarea. Acest lucru este necesar doar la instalare.

- Pe endpoint-urile Windows, este necesar ca link-urile din local spre local să fie activate.

Agent de securitate cu rol de protecție Exchange

În cazul Serverelor Exchange, carantina necesită spațiu suplimentar pe hard-disk, pe partiția pe care este instalat agentul de securitate.

Dimensiunea carantinei depinde de numărul de articole stocate și de dimensiunea acestora.

În mod implicit, agentul este instalat pe partiția sistemului.

Agent de securitate cu rol de server de memorie cache pentru patch-uri

Agentul cu rol de server de memorie cache pentru patch-uri trebuie să îndeplinească următoarele cerințe cumulate:

- Toate cerințele hardware pentru agentul simplu de securitate (fără roluri)
- Toate cerințele hardware ale rolului de Releu
- În plus, este necesar un spațiu liber pe hard disk de 100 GB pentru stocarea patch-urilor descărcate

Important

Dacă doriți să salvați patch-urile pe o altă partiție decât cea pe care este instalat agentul, asigurați-vă că ambele partiții au spațiu liber suficient pe hard disk (100 GB); în caz contrar, agentul va întrerupe instalarea. Acest lucru este necesar doar la instalare.

4.2.2. Sisteme de operare suportate

Deskop Windows

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)

- Actualizarea Windows 10 din 10 octombrie 2018 (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7



Avertisment

Bitdefender nu oferă compatibilitate cu build-urile Windows Insider Program.

Tabletă Windows și programe incluse

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Server Windows

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2

- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Linux



Important

Endpoint-urile Linux folosesc licențe din numărul de licențe destinate sistemelor de operare tip server.

- Ubuntu 14.04 LTS sau mai recent
- Red Hat Enterprise Linux / CentOS 6.0 sau mai recent⁽²⁾
- SUSE Linux Enterprise Server 11 SP4 sau mai recent
- OpenSUSE Leap 42.x
- Fedora 25 sau mai recent⁽¹⁾
- Debian 8.0 sau mai recent
- Oracle Linux 6.3 sau superior
- Amazon Linux AMI 2016.09 sau mai recent
- Amazon Linux 2



Avertisment

(1) Pe Fedora 28 și versiunile ulterioare, Bitdefender Endpoint Security Tools are nevoie de instalarea manuală a pachetului `libnsl`, prin executarea următoarei comenzi:

```
sudo dnf install libnsl -y
```

(2) Pentru instalările minime ale CentOS, Bitdefender Endpoint Security Tools are nevoie de instalarea manuală a pachetului `libnsl`, prin executarea următoarei comenzi:

```
sudo yum install libnsl
```

Cerințe preliminare privind Active Directory

La integrarea endpoint-urilor Linux cu un domeniu Active Directory prin System Security Services Daemon (SSSD), asigurați-vă că instrumentele **ldbsearch**,

krb5-user, și **krb5-config** sunt instalate și că kerberos este configurat corespunzător.

```
/etc/krb5.conf

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    default_realm = DOMAIN.NAME
    dns_lookup_realm = true
    dns_lookup_kdc = true
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    fcc-mit-ticketflags = true
    default_keytab_name = FILE:/etc/krb5.keytab

[realms]
    DOMAIN.NAME = {
        kdc = dc1.domain.name
        kdc = dc2.domain.name
        admin_server = dc.domain.com
        default_domain = domain.com
    }

[domain_realm]
    domain.name = DOMAIN.NAME
    .domain.name = DOMAIN.NAME

[appdefaults]
    pam = {
        debug = false
```

```
ticket_lifetime = 36000
renew_lifetime = 36000
forwardable = true
krb4_convert = false
}
```



Notă

Toate înregistrările sunt sensibile la grafia cu majuscule sau minuscule.

Compatibilitate cu scanarea la accesare


Scanarea la accesare este disponibilă pentru toate sistemele de operare găzduite acceptate. Pe sistemele Linux, asistența pentru scanarea la accesare este asigurată în următoarele situații:

Versiuni kernel	Distribuții Linux	Cerințe privind scanarea la accesare
2.6.38 sau mai recent*	Red Hat Enterprise Linux / CentOS 6.0 sau mai recent Ubuntu 14.04 sau mai recent SUSE Linux Enterprise Server 11 SP4 sau mai recent OpenSUSE Leap 42.x Fedora 25 sau mai recent Debian 9.0 sau mai recent Oracle Linux 6.3 sau superior Amazon Linux AMI 2016.09 sau mai recent	Trebuie să fie activată funcția (opțiunea kernel) Fanotify .
2.6.38 sau peste	Debian 8	Fanotify trebuie să fie activată și setată pe modul de aplicare, iar apoi trebuie recompilat pachetul kernel. Pentru detalii, consultați acest articol KB .

Versiuni kernel	Distribuții Linux	Cerințe privind scanarea la accesare
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender oferă asistență prin DazukoFS cu modulele pentru kernel precompilate.
Toate celelalte tipuri de kernel	Toate celelalte sisteme suportate	Modulul DazukoFS trebuie să fie compilat manual. Pentru mai multe detalii, vă rugăm consultați „ Compilarea manuală a modulului DazukoFS ” (p. 58).

* Cu anumite limitări, descrise mai jos.

Limitări privind scanarea la accesare

Versiuni kernel	Distribuții Linux	Detalii
2.6.38 sau peste	Toate sistemele compatibile	<p>Scanarea la accesare monitorizează locațiile partajate în rețea numai în următoarele condiții:</p> <ul style="list-style-type: none"> • Funcția Fanotify este activată atât pe sistemele de la distanță, cât și pe cele locale. • Partajarea se bazează pe sisteme de fișiere CIFS și NFS. <p> Notă Scanarea la accesare nu scanează locații partajate în rețea montate prin SSH sau FTP.</p>
Toate kernel-urile	Toate sistemele compatibile	Scanarea la accesare nu este suportată pe sistemele cu DazukoFS în cazul locațiilor partajate în rețea montate pe căi protejate deja de modulul de scanare la accesare.

Asistență Detecție și răspuns pentru stațiile de lucru (EDR - Endpoint Detection and Response)

Accesați [această pagină web](#) pentru o listă completă și actualizată a versiunilor de kernel și distribuții Linux care sunt compatibile cu Senzorul EDR.

macOS

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Modulul Control conținut nu este compatibil cu macOS Big Sur (11.0).

4.2.3. Sisteme de fișiere acceptate

Bitdefender se instalează pe și protejează următoarele sisteme de fișiere:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

Notă

Opțiunea de scanare la accesare nu este disponibilă pentru NFS și CIFS/SMB.

4.2.4. Browsere compatibile

Securitatea pentru browser Endpoint este testată pentru compatibilitatea cu următoarele browsere:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

4.2.5. Security Server

Security Server este o mașină virtuală preconfigurată care rulează pe un Server Ubuntu 12.04 LTS (kernel 3.2).

Notă

Este posibil ca licența dumneavoastră să nu includă această caracteristică.

Platforme de virtualizare

Bitdefender Security Server poate fi instalat pe următoarele platforme virtuale:

- VMware vSphere și vCenter Server 7.0, 6.7 actualizare 3, actualizare 2a, 6.7 actualizare 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

Notă

Funcționalitatea de Gestionare a volumului de lucru în vSphere 7.0 nu este compatibilă.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (inclusiv Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 sau Windows Server 2008 R2, 2012, 2012 R2 (inclusiv Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (inclusiv KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism cu AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism cu AOS 5.6, 5.11 STS
- Nutanix Prism cu AHV 20170830.115, 20170830.301 și 20170830.395 Community Edition

- Nutanix Prism versiunea 2018.01.31 (Community Edition)



Notă

Suport pentru alte platforme de virtualizare disponibil la cerere.

Memorie și CPU

Alocarea resurselor memoriei și CPU pentru Security Server depinde de numărul și tipul de mașini virtuale care rulează pe sistemul gazdă. Tabelul următor include resursele recomandate care trebuie alocate:

Număr de MV protejate	RAM	CPU
1-50 MV	2 GB	2 CPU
51-100 MV	2 GB	4 CPU
101-200 MV	4 GB	6 CPU

Spațiu HDD

Trebuie să asigurați un spațiu de 8 GB pe discul fiecărei gazde Security Server.

Distribuția Security Server pe sistemele gazdă

Deși nu este obligatorie, Bitdefender recomandă instalarea Security Server pe fiecare gazdă fizică, pentru performanțe superioare.

Latența rețelei

Latența comunicării dintre Security Server și endpoint-urile protejate trebuie să fie mai mică de 50 ms.

Nivelul de încărcare al modulului Protecție spațiu de stocare

4.2.6. Utilizarea pentru trafic

- **Traficul de actualizare a produselor între clientul stației de lucru și serverul de actualizări**

Fiecare update periodic de Bitdefender Endpoint Security Tools generează următorul trafic de download pe fiecare stație de lucru protejată:

- Pe SO Windows: ~20 MB

- Pe SO Linux: ~26 MB
- Pe macOS: ~25 MB
- **Traficul de actualizări de conținut de securitate descărcate între stația de lucru client și Serverul de actualizări (MB/zi)**

Tipul serverului de actualizări	Tipul motorului de scanare		
	Local	Hibrid	Central.
Relay	65	58	55
Serverul public de actualizări Bitdefender	3	3.5	3

- **Traficul de Scanare centralizată între clientul stației de lucru și Security Server**

Obiecte scanate	Tip Trafic		Descărcare (MB)	Încărcare (MB)
Fișiere*	Prima scanare		27	841
	Scanare cache		13	382
Site-uri internet**	Prima scanare	Trafic internet	621	N/A
		Security Server	54	1050
	Scanare cache	Trafic internet	654	N/A
		Security Server	0.2	0.5

* Datele furnizate au fost măsurate pentru 3,49 GB de fișiere(6.658 de fișiere), din care 1,16 GB sunt fișiere Portable Executable (PE).

** Datele furnizate au fost evaluate pentru cele mai importante 500 de site-uri.

- **Trafic de scanare hibrid între clientul stației de lucru și Serviciile Cloud Bitdefender**

Obiecte scanate	Tip Trafic	Descărcare (MB)	Încărcare (MB)
Fișiere*	Prima scanare	1.7	0.6
	Scanare cache	0.6	0.3
Trafic internet**	Trafic internet	650	N/A

Obiecte scanate	Tip Trafic	Descărcare (MB)	Încărcare (MB)
	Servicii Cloud Bitdefender	2.6	2.7

* Datele furnizate au fost măsurate pentru 3,49 GB de fișiere (6.658 de fișiere), din care 1,16 GB sunt fișiere Portable Executable (PE).

** Datele furnizate au fost evaluate pentru cele mai importante 500 de site-uri.



Notă

Timpul de așteptare în rețea între clientul stației de lucru și Serverul Cloud Bitdefender trebuie să fie sub 1 secundă.

- **Traficul dintre clienții Bitdefender Endpoint Security Tools Relay și serverul de actualizări pentru descărcarea conținutului de securitate**

Clienții cu rol Bitdefender Endpoint Security Tools Relay descarcă ~16 MB / zi* de pe serverul de actualizări.

* Disponibil pentru clienții Bitdefender Endpoint Security Tools începând de la versiunea 6.2.3.569.

- **Traficul dintre clienții stației de lucru și consola internet Control Center**

Între clienții stațiilor de lucru și consola internet Control Center se generează un trafic mediu de 618 KB / zi.

4.3. Protecție Exchange

Security for Exchange este oferit prin Bitdefender Endpoint Security Tools, care poate proteja atât sistemul de fișiere cât și serverul de e-mail Microsoft Exchange.

4.3.1. Medii compatibile Microsoft Exchange

Security for Exchange suportă următoarele versiuni și roluri Microsoft Exchange:

- Exchange Server 2019 cu rol de Edge Transport sau Mailbox
- Exchange Server 2016 cu rol de Edge Transport sau Mailbox
- Exchange Server 2013 cu rol de Edge Transport sau Mailbox
- Exchange Server 2010 cu rol de Edge Transport, Hub Transport sau Mailbox
- Exchange Server 2007 cu rol de Edge Transport, Hub Transport sau Mailbox

Security for Exchange este compatibil cu grupurile Database Availability Groups (DAG) Microsoft Exchange.

4.3.2. Cerințe de sistem

Security for Exchange este compatibil cu orice server fizic sau virtual de 64 de biți (Intel sau AMD) ce rulează o versiune și un rol compatibil Microsoft Exchange Server. Pentru detalii cu privire la cerințele de sistem pentru Bitdefender Endpoint Security Tools, consultați „[Agentul de securitate fără roluri](#)” (p. 17).

Disponibilitatea recomandată a resurselor serverului:

- Memorie RAM disponibilă: 1 GB
- Spațiu liber pe hard disk: 1 GB

4.3.3. Alte cerințe software

- Pentru Microsoft Exchange Server 2013 cu Service Pack 1: [KB2938053](#) de la Microsoft.
- Pentru Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 sau mai nou

4.4. Full Disk Encryption

GravityZone Full Disk Encryption vă permite să operați BitLocker pe endpoint-urile Windows și FileVault și utilitarul diskutil de tip linie de comandă pe endpoint-urile macOS prin intermediul Control Center.

Pentru a asigura protecția datelor, acest modul asigură criptarea integrală a unității de disc pentru volumele boot și non-boot, pe discuri fixe, și stochează cheile de recuperare în cazul în care utilizatorii își uită parola.

Modulul de criptare folosește resursele hardware existente din mediul dumneavoastră GravityZone.

În ceea ce privește software-ul, cerințele sunt aproximativ aceleași ca și pentru BitLocker, FileVault și utilitarul diskutil de tip linie de comandă, majoritatea limitărilor referindu-se la aceste instrumente.

Pe Windows

Modulul de criptare GravityZone suportă BitLocker, începând cu versiunea 1.2, pe mașinile cu sau fără cip TPM (Trusted Platform Module).

GravityZone suportă BitLocker pe stațiile de lucru care rulează următoarele sisteme de operare:

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (cu TPM)
- Windows 7 Enterprise (cu TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (cu TPM)

*BitLocker nu este inclus în aceste sisteme de operare și trebuie instalat separat. Pentru mai multe informații despre instalarea BitLocker pe Windows Server, consultați aceste articole KB furnizate de Microsoft:

- <https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server>
- [https://technet.microsoft.com/en-us/library/cc732725\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx)



Important

GravityZone nu suportă criptarea pe Windows 7 și Windows 2008 R2 fără TPM.

Pentru cerințe detaliate referitoare la BitLocker, consultați acest articol KB furnizat de Microsoft: [https://technet.microsoft.com/en-us/library/cc766200\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx)

Pe Mac

GravityZone suportă FileVault și diskutil pe stațiile de lucru macOS care rulează următoarele sisteme de operare:

- macOS Big Sur (11.0)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

4.5. Porturile de comunicare GravityZone

GravityZone este o soluție distribuită, ceea ce înseamnă că toate componentele sale comunică între ele utilizând rețeaua locală sau internetul. Fiecare componentă utilizează o serie de porturi pentru a comunica cu celelalte. Este necesar să vă asigurați că aceste porturi sunt deschise pentru GravityZone.

Pentru informații detaliate privind porturile GravityZone, consultați [acest articol KB](#).

5. INSTALAREA PROTECȚIEI

Pentru a proteja rețeaua cu Bitdefender, trebuie să instalați agenții de securitate GravityZone pe stațiile de lucru. În acest scop, aveți nevoie de un utilizator GravityZone Control Center cu drepturi de administrator pentru endpoint-urile pe care le administrați.

5.1. Administrarea licenței

GravityZone este licențiat prin intermediul unei singure chei pentru toate serviciile de securitate, cu excepția modulului Full Disk Encryption, care este livrat cu o cheie separată în cazul licenței anuale.

Puteți încerca gratuit GravityZone pentru o perioadă de 30 de zile. În timpul perioadei de evaluare, toate funcțiile sunt disponibile integral și puteți utiliza serviciul pe un număr nelimitat de calculatoare. Înainte de expirarea perioadei de evaluare, dacă doriți să continuați utilizarea serviciilor, trebuie să optați pentru un plan de licență contra cost și să-l achiziționați.

Pentru achiziționarea unei licențe, contactați un distribuitor Bitdefender sau contactați-ne prin e-mail la enterprisesales@bitdefender.com.

5.1.1. Găsirea unui distribuitor

Distribuitorii noștri vă vor oferi asistență cu privire la toate informațiile necesare și vă vor ajuta să alegeți cea mai bună opțiune de licențiere.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergeți în pagina [Localizare parteneri](#) din site-ul Bitdefender.
2. Selectați țara dvs. de reședință pentru a vizualiza informațiile de contact ale partenerilor Bitdefender disponibili.
3. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa enterprisesales@bitdefender.com.

5.1.2. Activarea licenței

Atunci când achiziționați un plan de licență pentru prima dată, vi se emite un cod de licență. Licența GravityZone este activată prin activarea acestui cod de licență.



Avertisment

Activarea unei licențe nu anexează caracteristicile asociate acesteia la licența activă la momentul respectiv. Noua licență se suprapune peste cea veche. De exemplu,

activarea unei licențe pentru 10 stații de lucru peste o licență pentru 100 de stații de lucru NU va rezulta în licențierea a 110 stații de lucru. Din contră, aceasta va reduce numărul de stații de lucru acoperite de la 100 la 10.

Codul de licență vă este transmis prin e-mail la momentul achiziționării. În funcție de nivelul de servicii contractat, odată ce codul dumneavoastră de licență este emis, furnizorul de servicii îl poate activa pentru dumneavoastră. Alternativ, puteți activa chiar dumneavoastră licența în mod manual, urmând acești pași:

1. Autentificați-vă în Control Center utilizând contul dumneavoastră.
2. Faceți clic pe numele de utilizator din colțul din dreapta sus al consolei și selectați **Compania mea**.
3. Verificați detaliile licenței curente în secțiunea **Licență**.
4. În secțiunea **Licență**, selectați tipul de **Licență**.
5. În câmpul **Cheie de licență**, introduceți cheia dumneavoastră de licență.
6. Faceți clic pe butonul **Verificare** și așteptați până când Control Center extrage informațiile despre cheia de licență introdusă.
7. Faceți clic pe **Save**.

5.1.3. Verificare detalii licență curentă în curs

Pentru vizualizarea detaliilor unei licențe:

1. Autentificați-vă în Control Center folosind un cont de partener sau administrator de organizație.
2. Faceți clic pe numele de utilizator din colțul din dreapta sus al consolei și selectați **Compania mea**.
3. Verificați detaliile licenței curente în secțiunea **Licență**. De asemenea, puteți face clic pe butonul **Verificare** și așteptați până când Control Center extrage cele mai recente informații despre codul de licență curent.

5.2. Instalarea Endpoint Protection

În funcție de configurația stației și de mediul de rețea, puteți alege să instalați doar agenții de securitate sau să folosiți și un **Security Server**. În cel de-al doilea caz, va trebui să instalați mai întâi Security Server și apoi agenții de securitate.

Pentru stații cu resurse hardware limitate, se recomandă folosirea Security Server.



Important

Doar Bitdefender Endpoint Security Tools este compatibil pentru conectarea la un Security Server. Pentru mai multe informații, consultați capitolul „[Arhitectura GravityZone](#)” (p. 9).

5.2.1. Instalarea Security Server

Security Server este o mașină virtuală dedicată care anulează duplicatale și centralizează majoritatea funcțiilor contra programelor periculoase ale clienților antimalware, acționând ca și server de scanare.



Notă

Este posibil ca licența dumneavoastră să nu includă această caracteristică.

Trebuie să instalați Security Server pe una sau mai multe gazde pentru a include numărul de mașini virtuale care trebuie protejate.


Trebuie să aveți în vedere numărul de mașini virtuale protejate, resursele disponibile pentru Security Server pe gazde, precum și conectivitatea în rețea dintre Security Server și mașinile virtuale protejate.

Agentul de securitate instalat pe mașinile virtuale se conectează la Security Server prin TCP/IP, folosind detalii configurate la instalare sau printr-o poliță.

Pachetul Security Server poate fi descărcat de pe Control Center în mai multe formate diferite, compatibile cu principalele platforme de virtualizare.

Descărcarea Pachetelor de instalare Security Server

Pentru a descărca pachetele de instalare Security Server:

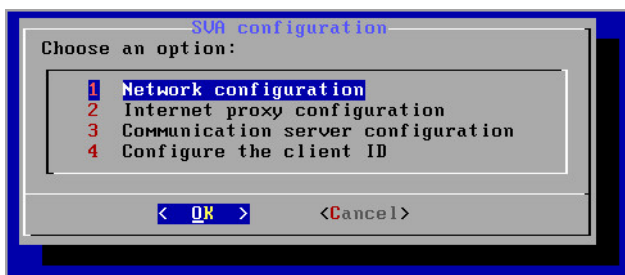
1. Mergeți la pagina **Rețea > Pachete**.
2. Selectați pachetul Security Server implicit:
3. Faceți clic pe butonul  **Descărcare** din partea de sus a tabelului și alegeți tipul de pachet din meniu.
4. Salvați pachetele selectate în locația dorită.

Executarea pachetelor de instalare Security Server

După ce aveți pachetul de instalare, configurați-l pe gazdă folosind instrumentul preferat de configurare a mașinii virtuale.

După configurare, setați Security Server după cum urmează:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere). Alternativ, vă puteți conecta la aplicație prin SSH.
2. Conectați-vă folosind datele implicite.
 - Nume de utilizator: root
 - Parolă: sve
3. Rulați comanda `sva-setup`. Veți accesa interfața de configurare a aplicației.



Interfața de configurare Security Server (meniu principal)

Pentru a naviga prin meniuri și opțiuni, folosiți tasta Tab tastele săgeți. Pentru a selecta o anumită opțiune, apăsați Enter.

4. Configurați setările rețelei.

Security Server folosește protocolul TCP/IP pentru comunicarea cu componentele GravityZone. Puteți configura aplicația pentru a obține automat setările rețelei de la serverul DHCP sau puteți configura manual setările rețelei, în modul descris mai jos:

 - a. Din meniul principal, selectați **Configurare rețea**.
 - b. Selectați interfața de rețea.
 - c. Selectați modul de configurare IP:
 - **DHCP**, dacă doriți ca Security Server să obțină automat setările de rețea de la serverul DHCP.
 - **Static**, dacă un server DHCP este absent sau dacă s-a efectuat o rezervare IP pentru aplicație pe serverul DHCP. În acest caz, trebuie să configurați manual setările de rețea.

- i. Introduceți numele gazdei, adresa IP, masca de rețea, portalul și serverele DNS în câmpurile corespunzătoare.
- ii. Selectați **OK** pentru a salva modificările.

**Notă**

Dacă sunteți conectat la aplicație prin clientul SSH, modificarea setărilor de rețea va încheia imediat sesiunea.

5. Configurați setările proxy.

Dacă în rețea se utilizează un server proxy, trebuie să furnizați detaliile acestuia, astfel încât Security Server să poată comunica cu GravityZone Control Center.

**Notă**

Sunt acceptate doar serverele proxy cu date de autentificare de bază.

- a. Din meniul principal, selectați **Configurare proxy internet**.
 - b. Introduceți numele gazdei, numele de utilizator, parola și domeniul în câmpurile corespunzătoare.
 - c. Selectați **OK** pentru a salva modificările.
- 6. Configurați adresa Serverului de comunicare.**
- a. Din meniul principal, selectați **Configurare server comunicare**.
 - b. Introduceți una dintre următoarele adrese pentru Serverul de comunicare:
 - <https://cloud-ecs.gravityzone.bitdefender.com:443>
 - <https://cloudgz-ecs.gravityzone.bitdefender.com:443>

**Important**

Această adresă trebuie să fie aceeași cu cea din setările politicii Control Center. Pentru a verifica link-ul, mergeți la pagina **Politici** și adăugați sau deschideți o politică adaptată, navigați la secțiunea **General > Comunicare > Alocare comunicare terminal** și introduceți numele Serverului de comunicare în câmpul de titlu. Serverul corect va fi afișat în rezultatele de căutare.

- c. Selectați **OK** pentru a salva modificările.
- 7. Configurați ID-ul clientului.**

- a. Din meniul principal, selectați **Configurare ID client**.
- b. Introduceți ID-ul companiei.
ID-ul este un șir de 32 de caractere pe care îl puteți găsi accesând pagina cu detaliile companiei în Control Center.
- c. Selectați **OK** pentru a salva modificările.

5.2.2. Instalarea agenților de securitate

Pentru a vă proteja stațiile de lucru fizice și virtuale, trebuie să instalați un agent de securitate pe fiecare dintre acestea. Pe lângă administrarea protecției protecției pe punctul de lucru local, agentul de securitate comunică și cu Control Center pentru primirea comenzilor administratorului și pentru transmiterea rezultatelor acțiunilor sale.

Pentru a afla mai multe despre agenții de securitate disponibili, consultați „[Agenți de securitate](#)” (p. 9).

Pe mașinile Windows și Linux, agentul de securitate poate avea două roluri și îl puteți instala după cum urmează:

1. Ca agent de securitate simplu pentru stațiile de lucru.
2. Ca **Releu**, acționând ca și agent de securitate și ca șiserver de comunicare, proxy și de actualizare pentru alte stații de lucru din rețea.



Avertisment

- Prima stație de lucru pe care instalați protecția trebuie să aibă rol de Releu, altfel nu veți putea instala de la distanță agentul de securitate pe celelalte stații de lucru din aceeași rețea.
- Stația de lucru Releu trebuie să fie pornită pentru ca agenții conectați să comunice cu Control Center.

Puteți instala agenții de securitate pe stații de lucru fizice și virtuale [rulând pachetele de instalare local](#) sau [prin executarea sarcinilor de instalare de la distanță](#) de pe Control Center.

Este foarte important să citiți cu atenție și să urmați instrucțiunile de pregătire a instalării.

În modul normal, agenții de securitate au o interfață de utilizator minimă. Permite utilizatorilor doar să verifice starea de protecție și să ruleze sarcini de securitate de bază (actualizări și scanări), fără a oferi acces la setări.

Dacă este activat de către administratorul de rețea prin intermediul pachetului de instalare și politicii de securitate, agentul de securitate poate rula și în **modul Utilizator privilegiat** pe stațiile de lucru Windows, permițând utilizatoului stației de lucru să vizualizeze și să modifice setările politicii. Cu toate acestea, administratorul Control Center poate controla în orice moment ce politici de securitate se aplică, având prioritate față de modul de Utilizator privilegiat.

În mod implicit, limba de afișare pentru interfața utilizatorului de pe stațiile de lucru Windows protejate este setată la momentul instalării, în funcție de limba contului dumneavoastră GravityZone.

Pe Mac, limba de afișare pentru interfața utilizatorului este setată la momentul instalării, în funcție de limba sistemului de operare al stației de lucru. În Linux, agentul de securitate nu are o interfață de utilizator localizată.

Pentru a instala interfața pentru utilizator în altă limbă pe anumite stații de lucru Windows, puteți crea un pachet de instalare și seta limba preferată în opțiunile de configurare ale acestuia. Această opțiune nu este disponibilă pentru stațiile de lucru Mac și Linux. Pentru mai multe informații cu privire la crearea pachetelor de instalare, consultați „[Generarea pachetelor de instalare](#)” (p. 43).

Pregătirea pentru instalare

Înainte de instalare, urmați pașii pregătitori de mai jos pentru a vă asigura că totul funcționează corect:

1. Asigurați-vă că toate stațiile de lucru țintă îndeplinesc **cerințele minime de sistem**. Pentru unele stații de lucru, se poate să fie necesară instalarea celui mai recent service pack disponibil sau eliberarea spațiului pe disc. Realizați o listă de stații de lucru care nu îndeplinesc cerințele necesare, pentru a le putea exclude din administrare.
2. Dezinstalați (nu doar dezactivați) orice program antimalware sau software de securitate Internet existent pe stațiile de lucru vizate. Rularea simultană a agentului de securitate cu alte aplicații pe o stație de lucru poate afecta funcționarea acestora și poate cauza probleme majore de sistem.

Multe dintre programele de securitate incompatibile sunt detectate automat și eliminate în momentul instalării.

Pentru a afla mai multe și pentru a verifica lista programelor software de securitate detectate de Bitdefender Endpoint Security Tools pentru sistemele de operare Windows actuale, consultați [acest articol din Baza de cunoștințe](#).



Important

Dacă doriți să instalați agentul de securitate pe un computer cu Bitdefender Antivirus for Mac 5.X, trebuie mai întâi să îl dezinstalați manual pe acesta din urmă. Pentru îndrumări, consultați [acest articol KB](#).

3. Pentru instalare este necesară existența privilegiilor de administrare și a accesului la Internet. În cazul în care stațiile de lucru vizate se află într-un domeniu Active Directory, trebuie să utilizați datele de autentificare ale administratorului domeniului pentru o instalare la distanță. În caz contrar, verificați dacă aveți la îndemână datele de autentificare necesare pentru toate stațiile de lucru.
4. Stațiile de lucru trebuie să aibă conectivitate la Control Center.
5. Se recomandă să folosiți o adresă IP statică pentru serverul releu. Dacă nu setați un IP static, folosiți numele de gazdă al mașinii.
6. La instalarea agentului prin intermediul unui releu Linux, trebuie respectate următoarele condiții suplimentare:
 - Endpoint-ul cu rol de Releu trebuie să aibă instalat pachetul Samba (`smbclient`) versiunea 4.1.0 sau mai recentă și să suporte comanda `net binary/command`, astfel încât să poată instala de la distanță agenți Windows.



Notă

De regulă, funcționalitatea `net binary/command` este livrată împreună cu pachetele `samba-client` și/sau `samba-common`. Pe anumite distribuții Linux (precum CentOS 7.4), comanda `net` se instalează numai în cazul instalării versiunii complete a suitei Samba (Common + Client + Server). Asigurați-vă că pe endpoint-ul cu rol de Releu este disponibilă comanda `net`.

- Stațiile de lucru Windows trebuie să aibă activate funcțiile Partajare administrativă și Partajare rețea.
 - Stațiile de lucru Linux și Mac vizate trebuie să aibă SSH activat.
7. Începând cu macOS High Sierra (10.13), după instalarea manuală sau de la distanță a Endpoint Security for Mac, utilizatorilor li se solicită să aprobe extensiile kernel Bitdefender pe computerele lor. Este posibil ca anumite caracteristici Endpoint Security for Mac să nu funcționeze până când utilizatorii nu aprobă extensiile kernel Bitdefender. Pentru a elimina intervenția utilizatorului, puteți pre-aproba extensiile kernel ale Bitdefender prin adăugarea lor în lista de excepții utilizând un instrument de administrare a dispozitivelor mobile.

Instalare locală

O modalitate în care puteți instala agentul de securitate pe o stație de lucru este aceea de a rula local un pachet de instalare.

Puteți crea și gestiona pachetele de instalare în pagina **Rețea și pachete**.

Bitdefender GravityZone							
Panou de bord							
Rețea							
Pachete							
	Numere	Tip	Limbă	Description	Stare	Companie	
Sarcini	<input type="checkbox"/>	Security Server Virtual Appliance	Security Server	English	Security for Virtualized Environments Security Server	Prețuri pentru descărcare	GravityZone Cloud
Politici	<input type="checkbox"/>	Endpoint	BEST	Română		Prețuri pentru descărcare	BDF1
Rapoarte	<input type="checkbox"/>	Endpoint Package	BEST	English	en	Prețuri pentru descărcare	SC AAA SRL
Carantină	<input type="checkbox"/>	EPS	BEST	English	eps connect to cloud	Prețuri pentru descărcare	SC AAA SRL

Pagina pachete



Avertisment

- Prima mașină pe care instalați protecția trebuie să aibă rol de Releu, altfel nu veți putea instala agentul de securitate pe celelalte stații de lucru din rețea.
- Mașina Releu trebuie să fie pornită și online pentru ca aplicațiile client să comunice cu Control Center.

După ce ați instalat primul client, acesta va fi utilizat pentru a detecta alte stații de lucru din aceeași rețea, pe baza mecanismului de Descoperire rețea. Pentru informații detaliate referitoare la descoperirea rețelei, consultați „[Cum funcționează opțiunea de descoperire a rețelei](#)” (p. 60).

Pentru a instala local agentul de securitate pe o stație de lucru, urmați acești pași:

1. [Creați un pachet de instalare](#) conform necesităților dumneavoastră.



Notă

Pașul nu este obligatoriu dacă un pachet de instalare a fost deja creat pentru rețeaua de sub contul dumneavoastră.

2. [Descărcați pachetul de instalare](#) pe stația de lucru țintă.
Alternativ, puteți [trimite link-urile de descărcare a pachetului de instalare prin e-mail](#) mai multor utilizatori din rețeaua dumneavoastră.
3. [Executați pachetul de instalare](#) pe stația de lucru țintă.

Generarea pachetelor de instalare

Fiecare pachet de instalare va fi vizibil în Control Center numai pentru partenerul care a creat pachetul și pentru conturile de utilizator subordonate companiei asociate pachetului de instalare.

Pentru a crea un pachet de instalare:

1. Conectați-vă și autentificați-vă la Control Center.
2. Mergeți la pagina **Rețea > Pachete**.
3. Dați clic pe butonul **+ Adăugare** situat în partea de sus a tabelului. Va apărea o fereastră de configurare.

Pachet nou stații de lucru ✕

General

Nume: *

Description:

Limbă: Română ▾

Companie: PABD ▾

Module:

- Antimalware
- Advanced Threat Control
- Firewall
- Control Conținut
- Control dispozitive
- Utiliz. privileg.

Roluri: Relay ⓘ Protecție Exchange ⓘ

Mod scanare ⓘ

Creare pachete - Opțiuni

4. Introduceți o denumire sugestivă și o descriere pentru pachetul de instalare pe care doriți să îl creați.
5. Din câmpul **Limbă**, selectați limba dorită pentru interfața clientului.

**Notă**

Această opțiune este disponibilă doar pentru sistemele de operare Windows.

6. Selectați modulele de protecție pe care doriți să le instalați.

**Notă**

Se vor instala doar modulele suportate pentru fiecare sistem de operare. Pentru mai multe informații, consultați capitolul „[Agenți de securitate](#)” (p. 9).

7. Selectați rolul stației de lucru țintă:

- **Releu**, pentru a crea pachetul pentru o stație de lucru cu rol de Releu. Pentru mai multe informații, consultați capitolul „[Relay](#)” (p. 11)
- **Server de cache pentru administrarea patch-urilor**, pentru a transforma releul într-un server intern pentru distribuirea patch-urilor software. Acest rol este afișat atunci când este selectat rolul de releu. Pentru mai multe informații, consultați capitolul „[Server de cache pentru patch-uri](#)” (p. 11)
- **Protecție Exchange**, pentru instalarea modulelor de protecție pentru serverele Microsoft Exchange, inclusiv funcțiile antimalware, antispam, filtrare conținut și atașamente pentru traficul de e-mail Exchange și scanare antimalware la cerere a bazelor de date Exchange. Pentru mai multe informații, consultați capitolul „[Instalarea Exchange Protection](#)” (p. 65).

8. Selectați compania unde se va utiliza pachetul de instalare.

9. **Eliminare concurență**. Se recomandă să selectați această casetă pentru a elimina automat orice software de securitate necompatibil în timp ce agentul Bitdefender se instalează pe endpoint. Prin deselectionarea acestei opțiuni, agentul Bitdefender se va instala alături de soluția de securitate existentă. Puteți elimina manual soluția de securitate instalată anterior mai târziu, cu propriul dvs. risc.

**Important**

Rularea simultană a agentului Bitdefender cu alte software-uri de securitate pe un endpoint le poate afecta funcționarea și poate cauza probleme majore în sistem.

10. **Mod scanare**. Alegeți tehnologia de scanare care se potrivește cel mai bine cu mediul de rețea și resursele stațiilor dvs. de lucru. Puteți defini modul de scanare selectând unul dintre următoarele tipuri:

- **Automat.** În acest caz, agentul de securitate va detecta automat configurația stației de lucru și va adapta în mod corespunzător tehnologia de scanare:
 - Scanare centralizată în cloud public sau privat (cu Security Server) cu fallback pe Scanare hibrid (motoare light), pentru calculatoarele fizice cu performanțe hardware scăzute și pentru mașinile virtuale. Acest caz necesită ca cel puțin un Security Server să fie instalat în rețea.
 - Scanare locală (cu motoare full) pentru calculatoarele fizice cu performanță hardware ridicată.



Notă

Calculatoarele cu performanță scăzută sunt considerate a avea frecvența procesorului mai mică decât 1.5 GHz sau memorie RAM mai mică decât 1 GB.

- **Personalizat.** În acest caz, puteți configura modul de scanare alegând între mai multe tipuri de tehnologii de scanare pentru mașini fizice și virtuale:
 - Scanare centralizată în cloud public sau privat (cu Security Server), care poate avea fallback* pe Scanarea locală (cu motoare full) sau Scanarea hibridă (cu motoare light).
 - Scanare hibrid (cu motoare light)
 - Scanare locală (cu motoare full)

Pentru instanțele EC2, puteți selecta unul dintre următoarele moduri de scanare personalizate:

Modul implicit de scanare pentru instanțele EC2 este Scanarea locală (conținutul de securitate este stocat pe agentul de securitate instalat, iar scanarea se execută local pe sistemul respectiv). Dacă doriți să scanați instanțele EC2 folosind un Security Server, este necesar să configurați în mod corespunzător pachetul de instalare al agentului de securitate și politica aplicată.





Modul implicit de scanare pentru mașinile virtuale Microsoft Azure este Scanarea locală (conținutul de securitate este stocat pe agentul de securitate instalat, iar scanarea se execută local pe sistemul respectiv). Dacă doriți să scanați mașinile virtuale Microsoft Azure folosind un Security Server, este necesar să configurați în mod corespunzător pachetul de instalare al agentului de securitate și politica aplicată.

- Scanare centralizată în cloud public sau privat (cu Security Server), care poate avea fallback* pe Scanarea hibrid (cu motoare light) sau Scanarea locală (cu motoare full).

* Atunci când se folosește scanarea cu motoare duble, dacă primul motor este indisponibil, se va folosi motorul de rezervă (fallback). Consumul de resurse și gradul de utilizare a rețelei vor depinde de motoarele folosite.

Pentru mai multe informații privind tehnologiile de scanare disponibile, consultați „[Motoare de scanare](#)” (p. 3)

11. Atunci când personalizați motoarele de scanare folosind scanarea în cloud-ul public sau privat (Security Server), vi se solicită să selectați serverele Security Server instalate local pe care doriți să le utilizați și să configurați prioritatea acestora în secțiunea **Alocare Security Server**:

- a. Dați clic pe lista Security Server din capătul de tabel. Se afișează lista de Security Server detectate.
- b. Selectați o entitate.
- c. Dați clic pe butonul  **Adăugare** din capătul de coloană **Acțiuni**.
Se adaugă Security Server în listă.
- d. Urmați aceiași pași pentru a adăuga mai multe servere de securitate, dacă sunt disponibile. În acest caz, le puteți configura prioritatea folosind săgețile  sus și  jos disponibile în partea dreaptă a fiecărei entități. Când primul Security Server nu este disponibil, va fi luat în considerare următorul și așa mai departe.
- e. Pentru a șterge o entitate din listă, dați clic pe butonul  **Ștergere** din partea de sus a tabelului.

Puteți alege să criptați conexiunea la Security Server selectând opțiunea **Utilizare SSL**.

12. Selectați **Scanare înainte de instalare** dacă doriți să vă asigurați că ați curățat mașinile înainte de a instala clientul pe acestea. Se va efectua o scanare rapidă în cloud pe mașinile vizate, înainte de pornirea instalării.
13. Bitdefender Endpoint Security Tools este instalat în directorul implicit de instalare. Selectați **Utilizare cale de instalare personalizată** dacă doriți să instalați agentul Bitdefender într-o altă locație. Dacă folderul specificat nu există, acesta va fi generat în timpul instalării.

- Pentru Windows, calea implicită este C:\Program Files\. Pentru a instala Bitdefender Endpoint Security Tools într-o locație personalizată, utilizați convențiile Windows la introducerea căii. Spre exemplu, D:\folder.
- Pentru Linux, Bitdefender Endpoint Security Tools este instalat implicit în directorul /opt. Pentru a instala agentul Bitdefender într-o locație personalizată, utilizați convențiile Linux la introducerea căii. Spre exemplu, /folder.

Bitdefender Endpoint Security Tools nu este compatibil cu instalarea în următoarele căi personalizate:

- Orice cale care nu începe cu slash (/). Singura excepție este locația Windows %PROGRAMFILES%, care este interpretată de agentul de securitate drept directorul implicit Linux /opt.
- Orice cale din /tmp sau /proc.
- Orice cale care conține următoarele caractere speciale: \$, !, *, ?, “, ‘, ` , \, (,), [,], {, }.
- Specificatorul de sistem systemd (%).

Pentru Linux, instalarea într-o cale personalizată necesită glibc 2.21 sau o versiune mai recentă.



Important

La utilizarea unei căi personalizate asigurați-vă că aveți pachetul corect de instalare pentru fiecare sistem de operare.

14. Dacă doriți, puteți seta o parolă pentru a împiedica utilizatorii să ștergă protecția. Selectați **Configurare parolă dezinstalare** și introduceți parola dorită în câmpurile corespunzătoare.
15. Dacă stațiile de lucru țintă sunt în Inventarul de rețea sub **Grupuri personalizate**, le puteți muta într-un anumit director imediat după finalizarea configurării agentului de securitate.
Selectați **Utilizare folder personalizat** și alegeți un folder din tabelul corespunzător.
16. În secțiunea **Agent de instalare**, alegeți entitatea la care se vor conecta stațiile de lucru țintă pentru instalarea și actualizarea clientului:
 - **Bitdefender Cloud**, dacă doriți să actualizați clienții direct de pe internet.

În acest caz, puteți defini, de asemenea, setările proxy dacă stațiile de lucru țintă se conectează la internet prin proxy. Selectați **Utilizare proxy pentru comunicații** și introduceți setările de proxy necesare în câmpurile de mai jos.

- **Relev Endpoint Security**, dacă doriți să conectați stațiile de lucru la un client de tip releu instalat în rețeaua dvs. Toate mașinile cu rolul de releu detectate în rețeaua dvs. vor fi afișate în tabelul afișat mai jos. Selectați mașina de tip releu dorită. Stațiile de lucru conectate vor comunica cu Control Center exclusiv prin releul specificat.



Important

Portul 7074 trebuie să fie deschis pentru ca instalarea prin Bitdefender Endpoint Security Tools Relay să funcționeze.

17. Faceți clic pe **Save**.

Pachetul nou creat va fi adăugat în lista de pachete ale companiei țintă.




Notă

Setările configurate în cadrul unui pachet de instalare se vor aplica pe stațiile de lucru imediat după instalare. Imediat după aplicarea politicii de securitate la nivelul clientului, setările configurate în cadrul politicii vor intra în vigoare, înlocuind anumite setări din pachetul de instalare (cum ar fi serverele de comunicații sau setările proxy).

Descărcați pachetele de instalare

Pentru a descărca pachetele de instalare ale agenților de securitate:

1. Înregistrați-vă în Control Center de pe stația de lucru pe care doriți să instalați protecția.
2. Mergeți la pagina **Rețea > Pachete**.
3. Selectați compania unde este situată stația de lucru din capătul de coloană **Companie**. Se vor afișa doar pachetele disponibile pentru compania selectată.
4. Selectați pachetul de instalare pe care doriți să îl descărcați.
5. Faceți clic pe butonul  **Descărcare** din partea de sus a tabelului și selectați tipul de instalare pe care doriți să o utilizați. Există două tipuri de fișiere de instalare:

- **Aplicație de descărcare.** Aplicația de descărcare descarcă mai întâi setul complet de instalare de pe serverele cloud ale Bitdefender și apoi demarează instalarea. Este de dimensiuni reduse și poate fi rulată atât pe sistemele de 32, cât și pe cele de 64 de biți (ceea ce ușurează distribuția). Dezavantajul este că necesită o conexiune activă la Internet.
- **Kit complet.** Kit-urile complete de instalare sunt mai mari și trebuie să ruleze pe un anumit tip de sistem de operare.

Setul complet va fi utilizat pentru a instala protecția pe stațiile de lucru cu o conexiune slabă sau chiar inexistentă la internet. Descărcați acest fișier pe o stație de lucru conectată la Internet și apoi distribuiți-l pe alte stații de lucru folosind un mediu de stocare extern sau un director partajat în rețea.



Notă

Versiuni cu kit complet disponibile:

- **Windows OS:** sisteme pe 32 de biți și pe 64 de biți
- **Linux OS:** sisteme pe 32 de biți și pe 64 de biți
- **macOS:** numai sisteme pe 64 de biți

Asigurați-vă că folosiți versiunea corectă pentru stația de lucru pe care instalați.

6. Salvați fișierul pe stația de lucru.



Avertisment

- Executabilul de descărcare nu trebuie redenumit. În caz contrar, nu veți putea descărca fișierele de instalare de pe serverul Bitdefender.


7. În plus, dacă ați ales Aplicația de descărcare, puteți crea un pachet MSI pentru stațiile de lucru Windows. Pentru informații suplimentare, consultați [acest articol KB](#).

Trimitere link-uri de descărcare pachete de instalare prin e-mail

Este posibil să trebuiască să informați rapid administratorii unei companii că pot descărca un pachet de instalare. În acest caz, urmați pașii de mai jos:

Este posibil să trebuiască să informați rapid ceilalți utilizatori că pot descărca un pachet de instalare. În acest caz, urmați pașii de mai jos:

1. Mergeți la pagina **Rețea > Pachete**.

2. Selectați pachetul de instalare dorit.
3. Faceți clic pe butonul  **Trimitere link-uri descărcare** din partea de sus a tabelului. Va apărea o fereastră de configurare.
4. Introduceți adresa de e-mail a fiecărui utilizator care urmează să primească link-ul de descărcare a pachetului de instalare. Apăsăți **Enter** după fiecare adresă de e-mail.
Asigurați-vă că fiecare adresă de e-mail introdusă este validă.
5. Dacă doriți să vizualizați link-urile de descărcare înainte de trimiterea acestora prin e-mail, faceți clic pe butonul **Link-uri de instalare**.
6. Faceți clic pe **Trimitere**. Un e-mail care conține link-ul de instalare este trimis fiecărei adrese de e-mail specificate.

Rularea pachetelor de instalare

Pentru ca instalarea să funcționeze, pachetul de instalare trebuie rulat folosind privilegiile de administrator.

Pachetul se instalează diferit pe fiecare sistem de operare, după cum urmează:

- Pe sistemele de operare Windows și macOS:
 1. Pe stația de lucru țintă, descărcați fișierul de instalare de pe Control Center sau copiați-l dintr-o unitate de partajare a rețelei.
 2. Dacă descărcați setul complet, extrageți fișierele din arhivă.
 3. Executați fișierul executabil.
 4. Urmați instrucțiunile de pe ecran.



Notă

Pe macOS, după instalarea Endpoint Security for Mac, utilizatorilor li se va solicita să aprobe extensiile kernel ale Bitdefender pe computerele lor. Anumite caracteristici ale agentului de securitate nu vor funcționa decât în momentul în care utilizatorii aprobă extensiile kernel ale Bitdefender. Pentru detalii, consultați [acest articol KB](#).

- Pe sistemele de operare Linux:
 1. Conectați-vă și autentificați-vă la Control Center.
 2. Descărcați sau copiați fișierul de instalare pe stația de lucru țintă.

3. Dacă descărcați setul complet, extrageți fișierele din arhivă.
4. Obțineți privilegiile de rădăcină executând comanda `sudo su`.
5. Modificați permisiunile asupra fișierului de instalare pentru a-l putea executa:

```
# chmod +x installer
```

6. Rulați fișierul de instalare:

```
# ./installer
```

7. Pentru a verifica dacă agentul a fost instalat pe stația de lucru, executați următoarea comandă:

```
$ service bd status
```

Duoă ce agentul de securitate a fost instalat, stația de lucru va apărea ca administrată în Control Center (pagina **Rețea**), în câteva minute.



Important

Dacă utilizați VMware Horizon View Persona Management, vă recomandăm să configurați Politica grupului activ de directoare pentru a exclude următoarele procese Bitdefender (fără calea completă):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Aceste excepții trebuie să fie aplicate atât timp cât agentul de securitate rulează la nivelul stației de lucru. Pentru detalii, consultați această [pagină cu documentație VMware Horizon](#).

Instalare de la distanță

Control Center vă permite să instalați de la distanță agentul de securitate pe stațiile de lucru detectate în rețea folosind sarcinile de instalare.

După ce ați efectuat instalarea locală pe primul client cu rol de Releu, este posibil să dureze câteva minute până când celelalte stații de lucru din rețea devin vizibile în Control Center. Din acest punct, puteți instala de la distanță agentul de securitate pe stațiile de lucru pe care le administrați folosind sarcinile de instalare din Control Center.

Bitdefender Endpoint Security Tools include un mecanism automat de descoperire a rețelei care permite detectarea altor stații de lucru din aceeași rețea. Stațiile de lucru detectate sunt afișate ca și **calculatoare neadministrate** din pagina **Rețea**.

Pentru a permite descoperirea rețelei, trebuie să aveți Bitdefender Endpoint Security Tools instalat deja pe cel puțin o stație de lucru din rețea. Această stație de lucru va fi utilizată pentru a scana rețeaua și a instala Bitdefender Endpoint Security Tools pe stațiile de lucru neprotejate.

Pentru informații detaliate referitoare la descoperirea rețelei, consultați „[Cum funcționează opțiunea de descoperire a rețelei](#)” (p. 60).

Cerințe pentru instalarea de la distanță

Pentru ca instalarea de la distanță să funcționeze:

- Bitdefender Endpoint Security Tools Relay trebuie să fie instalat în rețeaua dvs.
- Pe Windows:
 - Trebuie activată partajarea administrativă `admin$`. Configurați fiecare stație de lucru vizată pentru ca aceasta să nu utilizeze partajarea avansată de fișiere.
 - Configurați funcția Controlul contului utilizatorului (UAC - User Account Control) în funcție de sistemul de operare care rulează pe stațiile de lucru vizate. În cazul în care stațiile de lucru sunt într-un domeniu Active Directory, puteți utiliza o politică de grup pentru a configura funcția Controlul contului utilizatorului. Pentru detalii, consultați [acest articol KB](#).
 - Dezactivați Firewall-ul Windows sau configurați-l pentru a permite traficul prin intermediul protocolului de Partajare fișiere și imprimante (File and Printer Sharing).

**Notă**

Implementarea la distanță funcționează doar pe sistemele de operare moderne, începând cu Windows 7 / Windows Server 2008 R2, pentru care Bitdefender acordă suport complet. Pentru mai multe informații, consultați capitolul „Sisteme de operare suportate” (p. 20).

- Pe Linux: trebuie activat SSH.
- Pe macOS: trebuie activate autentificarea de la distanță și partajarea fișierelor.


Rularea sarcinilor de instalare de la distanță

Pentru a rula o sarcină de instalare de la distanță:

1. Conectați-vă și autentificați-vă la Control Center.
2. Mergeți la pagina **Rețea**.
3. Selectați grupul dorit din fereastra din stânga. Entitățile din grupul selectat sunt afișate în tabelul din fereastra din dreapta.

**Notă**

Opțional, puteți aplica filtre pentru a afișa exclusiv stațiile de lucru neadministrare. Dați clic pe meniul **Filtre** și selectați următoarele opțiuni: **Neadministrat** din fila **Securitate** și **Toate obiectele recursiv** din fila **Adâncime**.

4. Selectați entitățile (stațiile de lucru sau grupurile de stații de lucru) pe care doriți să instalați protecția.
5. Faceți clic pe butonul  **Sarcini** din partea din dreapta sus a tabelului și selectați **Instalare**.

Se afișează asistentul **Instalare client**.

Instalarea Bitdefender Endpoint Security Tools din meniul Sarcini

6. În secțiunea **Opțiuni**, configurați timpul de instalare:

- **Acum**, pentru a lansa instalarea imediat.
- **Programat**, pentru a configura intervalul de recurență al instalării. În acest caz, selectați intervalul de timp dorit (orar, zilnic sau săptămânal) și configurați-l conform necesităților dvs.



Notă

De exemplu, dacă sunt necesare anumite operațiuni pe mașina țintă înainte de a instala clientul (cum ar fi deinstalarea altor aplicații și repornirea sistemului de operare), puteți programa sarcina de instalare să ruleze la fiecare 2 ore. Sarcina va începe pe fiecare mașină țintă la fiecare 2 ore până la finalizarea cu succes a instalării.

7. Dacă doriți ca stațiile de lucru țintă să fie repornite automat pentru finalizarea instalării, selectați **Repornire automată (dacă este necesar)**.
8. În secțiunea **Administrare date de autentificare**, specificați drepturile de administrare necesare pentru autentificarea de la distanță pe stațiile de lucru țintă. Puteți adăuga datele de autentificare introducând numele de utilizator și parola pentru fiecare sistem de operare țintă.



Important

Pentru stații de lucru cu sistem de operare Windows 8.1, este necesar să furnizați datele de autentificare ale contului de administrator încorporat sau ale unui cont de administrator de domeniu. Pentru mai multe informații, consultați [acest articol KB](#).

Pentru a adăuga datele SO necesare:


- a. Introduceți numele de utilizator și parola unui cont de administrator în câmpurile corespunzătoare din capul de tabel.

În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

Folosiți convențiile Windows la introducerea denumirii contului de utilizator:

- Pentru mașinile Active Directory folosiți următoarele sintaxe: `username@domain.com` și `domain\username`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`user@domain.com` și `domain\user`).
- Pentru mașinile din grupul de lucru, e suficient să introduceți numai numele de utilizator, fără numele grupului de lucru.

Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont.

- b. Faceți clic pe butonul  **Adăugare**. Contul este adăugat la lista de date de autentificare.



Notă

Datele specificate sunt salvate automat în secțiunea [Administrare date de autentificare](#), astfel încât nu trebuie să le reintroduceți. Pentru a accesa funcția de Administrare date de autentificare, nu trebuie decât să dați clic pe numele dvs. de utilizator din colțul din dreapta sus al consolei.



Important

Dacă datele de autentificare furnizate nu sunt valabile, instalarea aplicației client va eșua pe stațiile de lucru respective. Asigurați-vă că actualizați datele de autentificare pentru sistemul de operare introduse în funcționalitatea de Administrare date de autentificare atunci când acestea se schimbă pe stațiile de lucru țintă.

9. Selectați casețele corespunzătoare conturilor pe care doriți să le folosiți.



Notă

Dacă nu ați selectat datele de autentificare, se va afișa un mesaj de avertizare. Acest pas este obligatoriu pentru instalarea de la distanță a agentului de securitate pe stațiile de lucru.

10. În secțiunea **Agent de instalare**, configurați releul la care se vor conecta stațiile de lucru țintă pentru instalarea și actualizarea clientului:

- Toate mașinile cu rolul de releu detectate în rețeaua dvs. vor fi afișate în tabelul din secțiunea **Instalare**. Fiecare client nou trebuie să fie conectat la cel puțin un client de tip releu din aceeași rețea, care va servi ca server de comunicații și actualizare. Selectați releul pe care doriți să îl asociați stațiilor de lucru țintă. Stațiile de lucru conectate vor comunica cu Control Center exclusiv prin releul specificat.



Important

Portul 7074 trebuie să fie deschis pentru ca instalarea prin agentul releu să funcționeze.

The screenshot shows the 'Instalator' interface. At the top, there is a dropdown menu for 'Instalator:' with 'Endpoint Security Relay' selected. Below this is a table with the following columns: 'Nume', 'IP', 'Denumire server personaliz...', and 'Eticheta'. The table contains two rows of data:

Nume	IP	Denumire server personaliz...	Eticheta
CO_SUPA	192.168.0.183		N/A
FC-WIN7-X64-01	192.168.3.80		N/A

At the bottom of the interface, there is a pagination bar showing 'Prima pagină', 'Pagina 1 din 1', 'Ultima pagină', and '20' items. The text '2 obiecte' is also visible at the bottom right.

11. Trebuie să selectați un pachet de instalare pentru instalarea curentă. Dați clic pe lista **Utilizare pachet** și selectați pachetul de instalare dorit. Puteți găsi aici toate pachetele de instalare create anterior pentru contul dumneavoastră, precum și pachetul de instalare implicit disponibil în Control Center.

12. Dacă este necesar, puteți modifica o parte din setările pachetului de instalare făcând clic pe butonul **Personalizare** de lângă câmpul **Utilizare pachet**.

Setările pachetului de instalare vor apărea mai jos și veți putea efectua modificările de care aveți nevoie. Pentru a afla mai multe despre modificarea pachetului de instalare, consultați „[Generarea pachetelor de instalare](#)” (p. 43).

Dacă doriți să salvați modificările ca pachet nou, selectați opțiunea **Salvare ca pachete** situată în partea de jos a listei de setări a pachetului și introduceți o denumire pentru noul pachet de instalare.

13. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.



Important

Dacă utilizați VMware Horizon View Persona Management, vă recomandăm să configurați Politica grupului activ de directoare pentru a exclude următoarele procese Bitdefender (fără calea completă):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Aceste excepții trebuie să fie aplicate atât timp cât agentul de securitate rulează la nivelul stației de lucru. Pentru detalii, consultați această [pagină cu documentație VMware Horizon](#).

Pregătirea sistemelor Linux pentru scanarea la accesare

Bitdefender Endpoint Security Tools pentru Linux include funcția de scanare la accesare, care funcționează cu anumite distribuții Linux și versiuni de kernel. Pentru mai multe informații, consultați [cerințele de sistem](#).

În continuare veți afla cum să compilați manual modulul DazukoFS.

Compilarea manuală a modului DazukoFS

Urmați pașii de mai jos pentru a compila DazukoFS pentru versiunea de kernel a sistemului și apoi încărcați modulul:

1. Descărcați headerele de kernel corespunzătoare.

- Pe sistemele **Ubuntu**, executați comanda următoare:

```
$ sudo apt-get install linux-headers-`uname -r`
```

- Pe sistemele **RHEL/CentOS**, executați comanda următoare:

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. Pe sistemele **Ubuntu**, aveți nevoie de build-essential:

```
$ sudo apt-get install build-essential
```

3. Copiați și extrageți codul sursă DazukoFS în directorul preferat:

```
# mkdir temp
# cd temp
# cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
# tar -xzvf dazukofs-source.tar.gz
# cd dazukofs-3.1.4
```

4. Compilați modulul:

```
# make
```

5. Instalați și încărcați modulul:

```
# make dazukofs_install
```

Cerințele pentru utilizarea scanării la accesare cu DazukoFS

Pentru ca DazukoFS și scanarea la accesare să funcționeze bine împreună, trebuie să se îndeplinească o serie de condiții. Vă rugăm să verificați dacă oricare dintre afirmațiile de mai jos se aplică sistemului dumneavoastră Linux și să urmați instrucțiunile pentru a evita eventualele probleme.

- Politica SELinux trebuie să fie dezactivată sau setată pe nivelul **permisiv**. Pentru a verifica și ajusta setările politicii SELinux, editați fișierul `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools este compatibil exclusiv cu versiunea DazukoFS inclusă în pachetul de instalare. Dacă DazukoFS este deja instalat pe sistem, îndeplătați-l înainte de a instala Bitdefender Endpoint Security Tools.
- DazukoFS suportă doar anumite versiuni kernel. Dacă pachetul DazukoFS furnizat împreună cu Bitdefender Endpoint Security Tools nu este compatibil cu versiunea kernel a sistemului, încărcarea modulului nu va reuși. În acest caz puteți fie actualiza kernelul conform versiunii suportate sau puteți recompila modulul DazukoFS pentru versiunea dvs. de kernel. Puteți găsi pachetul DazukoFS în directorul de instalare Bitdefender Endpoint Security Tools:
`/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`
- Atunci când partajați fișiere folosind servere dedicate precum NFS, UNFSv3 sau Samba, trebuie să porniți serviciile în următoarea ordine:

1. Activați scanarea la accesare prin intermediul politicii din Control Center.

Pentru mai multe informații, consultați Ghidul Partenerului GravityZone sau Ghidul Administratorului.

2. Porniți serviciul de partajare în rețea.

Pentru NFS:

```
# service nfs start
```

Pentru UNFSv3:

```
# service unfs3 start
```

Pentru Samba:

```
# service smb start
```



Important

Pentru serviciul NFS, DazukoFS este compatibil doar cu serverul de utilizatori NFS User Server.

Cum funcționează opțiunea de descoperire a rețelei

În afara integrării cu Active Directory, GravityZone include și un mecanism automat de descoperire a rețelei, dedicat detectării calculatoarelor din grupul de lucru.

GravityZone se bazează pe serviciul **Microsoft Computer Browser** și pe instrumentul **NBTscan** pentru descoperirea rețelei.

Serviciul Computer Browser este o tehnologie de rețelistică utilizată de calculatoarele care rulează Windows pentru menținerea unei liste actualizate de domenii, grupuri de lucru și a calculatoarelor incluse în acestea și pentru furnizarea acestor liste către calculatoarele client, la cerere. Calculatoarele detectate în rețea de serviciul Computer Browser pot fi vizualizate prin rularea comenzii **net view** într-o fereastră de introducere a comenzii.

```
Z:\>net view
Server Name      Remark
-----
\\SCIREFDL
\\SCIREFJM
\\SCIREFL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

Comanda net view

Instrumentul NBTscan scanează rețelele calculatoarelor folosind NetBIOS. Acesta interoghează fiecare stație de lucru din rețea și extrage informații precum adresa IP, numele calculatorului NetBIOS și adresa MAC.

Pentru a permite descoperirea automată a rețelei, trebuie să aveți Bitdefender Endpoint Security Tools Relay instalat deja pe cel puțin o stație de lucru din rețea. Acest calculator va fi utilizat pentru scanarea rețelei.

! Important

Control Center nu utilizează informații privind rețeaua din Active Directory sau din funcția harta rețelei. Harta rețelei se bazează pe o altă tehnologie de descoperire a rețelei: protocolul Link Layer Topology Discovery (LLTD).

Control Center nu este implicată activ în funcționarea serviciului Computer Browser. Bitdefender Endpoint Security Tools interoghează doar serviciul Computer Browser pentru a obține lista de stații de lucru și servere vizibile la momentul respectiv în rețea (cunoscută sub numele de lista de navigare) și apoi o trimite către Control Center. Control Center procesează lista de parcurgere și include noile calculatoare detectate în lista **Calculatoare neadministrate**. Calculatoarele detectate anterior nu sunt șterse după o nouă interogare de descoperire a rețelei; prin urmare, trebuie să excludeți și să ștergeți manual & calculatoarele care nu mai sunt în rețea.

Interogarea inițială aferentă listei de parcurgere este efectuată de primul Bitdefender Endpoint Security Tools instalat în rețea.

- Dacă releul este instalat pe un calculator aparținând unui grup de lucru, numai calculatoarele din acest grup vor fi vizibile în Control Center.
- Dacă releul este instalat pe un calculator de domeniu, numai calculatoarele din domeniul respectiv vor fi vizibile în Control Center. Calculatoarele din alte domenii pot fi detectate dacă există o relație de încredere cu domeniul pe care este instalat releul.

Interogările ulterioare pentru descoperirea rețelei sunt efectuate regulat, în fiecare oră. Pentru fiecare nouă interogare, Control Center împarte spațiul calculatoarelor administrate în zonele de vizibilitate și apoi identifică un releu în fiecare zonă, pentru executarea sarcinii. O zonă de vizibilitate este un grup de calculatoare care se detectează reciproc. În general, o zonă de vizibilitate este definită de un grup de lucru sau domeniu, însă aceasta depinde de topologia și configurația rețelei. În anumite cazuri, o zonă de vizibilitate poate include mai multe domenii și grupuri de lucru.

Dacă un releu selectat nu efectuează interogarea, Control Center așteaptă până la următoarea interogare programată, fără a alege un alt releu pentru a relua încercarea.

Pentru vizibilitate completă a rețelei, releul trebuie instalat pe cel puțin un calculator din fiecare grup de lucru sau domeniu din rețeaua dumneavoastră. Ideal, Bitdefender Endpoint Security Tools trebuie instalat pe cel puțin un calculator din fiecare sub-rețea.

Mai multe despre serviciul Microsoft Computer Browser

Pe scurt despre serviciul Computer Browser:

- Operează independent de Active Directory.
- Rulează exclusiv pe rețelele IPv4 și operează independent în limitele unui grup LAN (grup de lucru sau domeniu). O listă de parcurgere este realizată și menținută pentru fiecare grup LAN.
- În mod tipic, utilizează pentru comunicarea între noduri transmisiile prin servere și nevalidate.
- Utilizează NetBIOS prin TCP/IP (NetBT).
- Necesită o rezoluție de nume NetBIOS. Se recomandă existența unei infrastructuri Windows Internet Name Service (WINS) care să ruleze în rețea.
- Nu este activată implicit pe Windows Server 2008 și 2008 R2.

Pentru informații detaliate privind serviciul Computer Browser, accesați [Computer Browser Service Technical Reference](#) de pe Microsoft Technet.

Cerințe pentru aplicația de descoperire a rețelei

Pentru descoperirea cu succes a tuturor calculatoarelor (servere și stații de lucru) care vor fi administrate de pe Control Center, sunt necesare următoarele:

- Calculatoarele trebuie să fie asociate într-un grup de lucru sau domeniu și conectate printr-o rețea locală IPv4. Serviciul Computer Browser nu funcționează pe rețelele IPv6.
- Mai multe calculatoare din fiecare grup LAN (grup de lucru sau domeniu) trebuie să ruleze serviciul Computer Browser. Controlerele principale ale domeniului trebuie să ruleze de asemenea serviciul.
- NetBIOS prin TCP/IP (NetBT) trebuie să fie activată pe calculatoare. Firewall-ul local trebuie să permită traficul NetBT.
- Dacă se utilizează un releu Linux pentru a descoperi alte stații de lucru Linux sau Mac, este necesar fie să instalați Samba pe stațiile de lucru țintă, fie să le uniți în Active Directory și să folosiți DHCP. În acest fel, NetBIOS va fi configurat automat pe acestea.
- Partajarea fișierelor trebuie să fie activată pe toate calculatoarele. Firewall-ul local trebuie să permită partajarea fișierelor.

- O infrastructură Windows Internet Name Service (WINS) trebuie să fie configurată și să funcționeze corespunzător.
- Funcția de descoperire a rețelei trebuie activată (**Control Panel >; Network and Sharing Center >; Change Advanced Sharing Settings**).
Pentru activarea acestei funcții, trebuie inițiate următoarele servicii:
 - DNS Client
 - Function Discovery Resource Publication
 - SSDP Discovery
 - UPnP Device Host
- În medii cu mai multe domenii, se recomandă configurarea unor relații de încredere între domenii, pentru a permite calculatoarelor să acceseze listele de parcurgere din alte domenii.

Calculatoarele de pe care Bitdefender Endpoint Security Tools interoghează serviciul Computer Browser trebuie să poată identifica numele NetBIOS.



Notă

Mecanismul de descoperire a rețelei funcționează pentru toate sistemele de operare acceptate, inclusiv versiunile de Windows Embedded, cu condiția să fie îndeplinite cerințele.

5.3. Instalarea EDR

Acest modul este livrat implicit cu setul de instalare Bitdefender Endpoint Security Tools și necesită activarea Sensorului de incidente la prima introducere a cheii de licență.

Înainte de instalări, asigurați-vă că endpoint-urile vizate îndeplinesc [cerințele minime](#). Cerințele minime pentru incidente corespund cerințelor agentului de securitate.

Pentru a vă proteja stațiile de lucru cu EDR, puteți selecta una dintre cele două opțiuni:

- Instalați agenții de securitate împreună cu Sensorul EDR atunci când introduceți cheia de licență. Consultați secțiunea [Activarea licenței](#).
- Utilizați sarcina **Reconfigurare**.



Important

The Incidents Sensor no longer provides support for Internet Explorer.

Pentru informații suplimentare, consultați Ghidul administratorului GravityZone.

5.4. Instalarea Full Disk Encryption

Full Disk Encryption se activează diferit pentru companiile client cu licențe lunare și anuale.

- Pentru [companiile client cu licență anuală](#), Full Disk Encryption este livrat sub formă de add-on, care necesită activarea pe baza unei chei de licență.
- Pentru [companiile client cu licență lunară](#), puteți permite administrarea Full Disk Encryption pentru fiecare companie, fără a furniza o cheie de licență.

Companiile client cu licență anuală

Pentru a activa Full Disk Encryption pentru companiile client cu licență anuală:

1. Conectați-vă la Control Center.
2. Accesați **Companii**.
3. Efectuați clic pe denumirea companiei pentru care doriți să activați Full Disk Encryption.
4. În secțiunea **Licență**, introduceți cheia de licență pentru Full Disk Encryption în câmpul **Cheie add-on**.
5. Faceți clic pe **Add**. Detaliile referitoare la add-on apar într-un tabel: tipul, cheia de licență și opțiunea de a șterge cheia.
6. Faceți clic pe **Salvare** pentru a aplica modificările.

Companiile client cu licență lunară

Pentru a permite administrarea Full Disk Encryption pentru companiile client cu licență lunară:

1. Conectați-vă la Control Center.
2. Accesați **Companii**.
3. Efectuați clic pe butonul **+ Adăugare** din bara de instrumente de acțiune.
4. Introduceți datele solicitate, selectați **Client** la tipul companiei și **Licență lunară** la tipul licenței.
5. Bifați caseta **Permite companiei să administreze criptarea**.
6. Faceți clic pe **Salvare** pentru a aplica modificările.

Companiile partenere au setările implicite pentru Full Disk Encryption și nu pot activa sau dezactiva această caracteristică.

Pentru informații detaliate cu privire la cheile de licență, consultați „[Administrarea licenței](#)” (p. 34).

Agenții de securitate Bitdefender suportă modulul Full Disk Encryption începând cu versiunea 6.2.22.916 pe Windows și 4.0.0173876 pe Mac. Pentru a vă asigura că agenții sunt pe deplin compatibili cu acest modul, aveți la dispoziție două opțiuni:

- Instalați agenții de securitate cu modulul de Criptare inclus.
- Utilizați sarcina **Reconfigurare**.

Pentru informații detaliate despre utilizarea modulului Full Disk Encryption în rețeaua dvs., consultați capitolul **Politici de securitate > Criptare** din Ghidul administratorului GravityZone.

5.5. Instalarea Exchange Protection

Security for Exchange se integrează automat cu serverele Exchange, în funcție de rolul serverului. Pentru fiecare rol sunt instalate doar caracteristicile compatibile, după cum este descris în continuare:

Funcționalități	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Edge	Mailbox	Edge	Hub	Mailbox
Nivel Transport					
Filtrare antimalware	x	x	x	x	
Filtrare Antispam	x	x	x	x	
Filtrare pe bază de conținut	x	x	x	x	
Filtrare atașamente	x	x	x	x	
Exchange Store					
Scanare antimalware la cerere		x			x

5.5.1. Pregătirea pentru instalare

Înainte de a instala Security for Exchange, asigurați-vă că toate [cerințele](#) sunt îndeplinite, în caz contrar este posibil ca Bitdefender Endpoint Security Tools să se instaleze fără modulul de Protecție Exchange.

Pentru ca modulul de Protecție Exchange să funcționeze fără probleme și să prevină apariția conflictelor și rezultatele nedorite, dezinstalați agenții antimalware și de filtrare e-mail.

Bitdefender Endpoint Security Tools detectează automat și dezinstalează majoritatea produselor antimalware, dezactivând agentul antimalware integrat în Exchange Server de la versiunea 2013. Pentru detalii privind lista de software-uri detectate, consultați [acest articol KB](#).

Puteți reactiva manual agentul antimalware Exchange integrat în orice moment, însă nu este recomandat să faceți acest lucru.

5.5.2. Instalarea protecției pe serverele Exchange

Pentru a proteja serverele Exchange, este necesar să instalați Bitdefender Endpoint Security Tools cu rol de Protecție Exchange pe fiecare dintre acestea.

Aveți mai multe opțiuni pentru configurarea Bitdefender Endpoint Security Tools pe serverele Exchange:

- Instalare locală, prin descărcarea și executare pachetului de instalare de pe server.
- Instalare de la distanță, prin executarea unei sarcini de **Instalare**.
- De la distanță, prin executarea sarcinii **Reconfigurare client**, dacă Bitdefender Endpoint Security Tools asigură deja protecția sistemului de fișiere de pe server.

Pentru a vedea pașii de instalare detaliați, consultați „[Instalarea agenților de securitate](#)” (p. 39).

5.6. Manager Credențiale

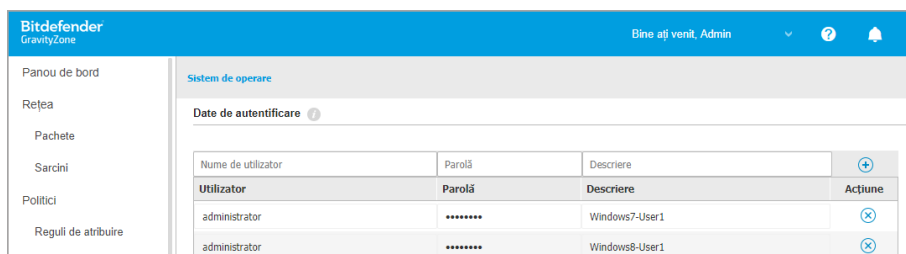
Secțiunea de Administrare date de autentificare vă ajută să definiți datele de autentificare necesare pentru autentificarea de la distanță pe diferite sisteme de operare din rețeaua dumneavoastră.

Pentru a deschide fereastra Administrare date de autentificare, faceți clic pe numele de utilizator din colțul din dreapta sus al paginii și selectați **Administrare date de autentificare**.

5.6.1. Adăugare de date în modulul Administrare Date de Autentificare

Cu secțiunea Administrare date de autentificare, puteți administra drepturile necesare pentru autentificarea de la distanță la executarea sarcinilor de instalare transmise calculatoarelor și mașinilor virtuale din rețea.

Pentru a adăuga un set de date de autentificare:



The screenshot shows the Bitdefender GravityZone web interface. The top navigation bar includes the logo, the text 'Bine ați venit, Admin', and icons for help and notifications. A left sidebar contains a menu with items like 'Panou de bord', 'Rețea', 'Pachete', 'Sarcini', 'Politici', and 'Reguli de atribuire'. The main content area is titled 'Sistem de operare' and contains a section for 'Date de autentificare'. This section features a table with columns for 'Utilizator', 'Parolă', 'Descriere', and 'Acțiune'. The table contains two rows of data, both for 'administrator' users on 'Windows7-User1' and 'Windows8-User1' systems. Each row has a plus icon for adding and a minus icon for deleting.

Utilizator	Parolă	Descriere	Acțiune
administrator	*****	Windows7-User1	⊕ ⊖
administrator	*****	Windows8-User1	⊕ ⊖

Manager Credențiale

1. Introduceți numele de utilizator și parola unui cont de administrator pentru fiecare sistem de operare țintă, în câmpurile corespunzătoare din partea de sus a capului de tabel. Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont. În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

Folosiți convențiile Windows la introducerea denumirii contului de utilizator:


- Pentru mașinile Active Directory folosiți următoarele sintaxe: `username@domain.com` și `domain\username`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`user@domain.com`, `username@domain.com` și `domain\userusername`).
 - Pentru mașinile din grupul de lucru, e suficient să introduceți numai numele de utilizator, fără numele grupului de lucru.
2. Faceți clic pe butonul **⊕ Adăugare** din dreapta tabelului. Noul set de date de autentificare este adăugat la tabel.

**Notă**

Dacă nu ați specificat datele de autentificare, vi se va solicita să le introduceți atunci când executați sarcinile de instalare. Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

5.6.2. Ștergerea datelor din fereastra Administrare Date de Autentificare

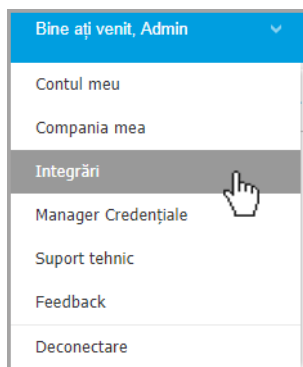
Pentru a șterge datele de autentificare care nu mai sunt valabile din fereastra Administrare date de autentificare:

1. Îndreptați cursorul către rândul din tabel care include datele pe care doriți să le ștergeți.
2. Faceți clic pe butonul  **Ștergere** din dreapta rândului corespunzător din tabel. Contul selectat va fi șters.

6. INTEGRĂRI

GravityZone oferă posibilitatea de a integra Control Center cu soluții terțe.

Puteți configura integrarea soluțiilor produse de terți în pagina **Integrări**, pe care o puteți accesa dând clic pe numele de utilizator din colțul din dreapta sus al consolei și selectând **Integrări**.



Din această pagină, puteți adăuga, modifica sau elimina integrările în funcție de nevoile dumneavoastră.

6.1. Integrare cu ConnectWise Automate

Cu această integrare, aveți acces la funcțiile GravityZone precum configurarea, gestionarea carantinei, alertele și notificările din Automate Control Center. Pentru mai multe informații, consultați [Ghidul de integrare ConnectWise Automate](#).

6.2. Integrare cu ConnectWise Manage

Control Center oferă o funcționalitate de integrare specifică pentru partenerii cu conturi ConnectWise, permițând monitorizarea eficientă a serviciilor de securitate ale Bitdefender furnizate companiilor client prin intermediul platformei ConnectWise, în baza procedurilor de emisie tichete și facturare automatizate.

Pentru informații complete cu privire la modul de integrare a consolei GravityZone Control Center cu Connect Manage, consultați [Ghidul de integrare Connect Manage](#).

6.3. Integrarea cu Amazon EC2

În calitate de furnizor de servicii administrate (MSP) cu cont de Partener în GravityZone Control Center, aveți posibilitatea de a integra Control Center cu Amazon EC2 și de a instala, gestiona și monitoriza în mod centralizat securitatea Bitdefender pe inventarul de instanțe aferent. Serverele de scanare brevetate sunt găzduite de Bitdefender în cloud-ul AWS pentru a asigura o amprentă optimă asupra instanțelor protejate și pentru a elimina supraîncărcarea la scanare care apare în cazul software-urilor de securitate tradiționale.

Pentru informații complete despre arhitectura Bitdefender Security for AWS, cerințe, abonare, crearea și administrarea integrării cu Amazon EC2, consultați [Ghidul de integrare cu Amazon EC2](#).

6.4. Integrarea cu Splunk

Partenerii cu conturi Splunk pot trimite date din GravityZone către Splunk prin HTTP Event Collector. Această integrare utilizează API-urile GravityZone, iar pentru configurare necesită acces simultan la Control Center și la platforma Splunk.

Pentru indicații complete cu privire la modul de integrare a GravityZone cu Splunk, consultați [acest articol KB](#).

6.5. Integrare cu Kaseya VSA

Prin această integrare puteți administra securitatea GravityZone din Kaseya VSA. Pentru mai multe informații, consultați [Ghidul de integrare Bitdefender Kaseya VSA](#).

6.6. Integrare cu Datto RMM

Prin această integrare, puteți configura agentul de securitate Bitdefender pe o țintă individuală sau pe multiple ținte. Pentru mai multe informații, consultați [Ghidul de utilizatorului pentru componentele Datto RMM](#).

7. DEZINSTALAREA PROTECȚIEI

Puteți dezinstala și reinstala componentele GravityZone în situații cum ar fi cea în care trebuie să folosiți un cod de licență pentru o altă stație, pentru a remedia erori sau pentru a trece la versiuni superioare.

Pentru a dezinstala corect protecția Bitdefender de pe stațiile de lucru din rețeaua dumneavoastră, urmați instrucțiunile descrise în acest capitol.

- [Dezinstalarea Endpoint Protection](#)
- [Dezinstalarea Exchange Protection](#)

7.1. Dezinstalarea Endpoint Protection

Pentru a șterge în siguranță protecția Bitdefender, trebuie să dezinstalați mai întâi agenții de securitate și apoi Security Server, dacă este necesar. Dacă doriți să dezinstalați doar Security Server, conectați mai întâi agenții acestuia la un alt Security Server.

- [Dezinstalarea agenților de securitate](#)
- [Dezinstalarea Security Server](#)

7.1.1. Dezinstalarea agenților de securitate

La dezinstalarea agenților de securitate, aveți două opțiuni:

- [De la distanță](#) în Control Center
- [Manual](#) pe stația țintă

Dezinstalarea de la distanță

Pentru a dezinstala protecția Bitdefender de pe orice terminal administrat de la distanță:

1. Mergiți la pagina **Rețea**.
2. Selectați containerul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați stațiile de lucru de pe care doriți să dezinstalați agentul de securitate Bitdefender.

4. Faceți clic pe **Sarcini** din partea de sus a tabelului și selectați **Dezinstalare client**. Este afișată o fereastră de configurare.
5. În fereastra de sarcini **Dezinstalare agent** puteți selecta dacă doriți să păstrați fișierele trecute în carantină pe stația de lucru sau să le ștergeți.
6. Faceți clic pe **Salvare** pentru a genera sarcina. Se va afișa un mesaj de confirmare.

Puteți vizualiza și administra sarcina în **Rețea > Sarcini**.

Dezinstalare locală

Pentru a dezinstala manual agentul de securitate Bitdefender de pe o stație Windows:

1. În funcție de sistemul de operare:
 - Pentru Windows 7, mergeți la **Start > Control Panel > Uninstall a program** din categoria **Programs**.
 - Pentru Windows 8, mergeți la **Settings > Control Panel > Uninstall a program** din categoria **Program**.
 - Pentru Windows 8.1, faceți clic dreapta pe butonul **Start**, apoi selectați **Control Panel > Programs & features**.
 - Pentru Windows 10, mergeți la **Start > Settings > System > Apps & features**.
2. Selectați agentul Bitdefender din lista programelor.
3. Faceți clic pe **Dezinstalare**.
4. Introduceți parola Bitdefender, dacă este activată în politica de securitate. În timpul instalării, puteți vizualiza progresul sarcinii.

Pentru a dezinstala manual agentul de securitate Bitdefender de pe o mașină Linux:

1. Deschideți terminalul.
2. Obțineți acces la rădăcină folosind comenzile `su` sau `sudo su`.
3. Navigați folosind comanda `cd` către calea următoare: `/opt/BitDefender/bin`
4. Rulați scriptul:

```
# ./remove-sve-client
```


5. Introduceți parola Bitdefender pentru a continua, dacă este activată în politica de securitate.


Pentru a dezinstala manual agentul Bitdefender de pe un Mac:

1. Mergeți la **Căutare > Aplicații**.
2. Deschideți directorul Bitdefender.
3. Faceți dublu clic pe **Dezinstalare Mac Bitdefender**.
4. În fereastra de confirmare, faceți clic pe **Verificare** și **Dezinstalare** pentru a continua.

7.1.2. Dezinstalarea Security Server

Pentru a îndepărta Security Server:

1. Opriți calculatorul și ștergeți mașina virtuală Security Server din mediul dumneavoastră de virtualizare.
2. Conectați-vă la GravityZone Control Center.
3. Mergeți la secțiunea **Rețea** și căutați Security Server în inventar. După o perioadă de la momentul în care ați șters mașina virtuală, Security Server va fi raportat ca fiind offline.
4. Selectați căsuța corespunzătoare pentru Security Server.
5. Efectuați clic pe butonul  **Ștergere** din bara de instrumente de acțiune.

Security Server va fi mutat în directorul **Șterse**, de unde îl puteți șterge definitiv prin efectuarea unui nou clic pe butonul  **Ștergere** din bara de instrumente de acțiune.

7.2. Dezinstalarea Exchange Protection

Puteți șterge Protecția Exchange de pe orice Server Microsoft Exchange cu Bitdefender Endpoint Security Tools cu acest rol instalat. Puteți efectua dezinstalarea din Control Center.

1. Mergeți la pagina **Rețea**.
2. Selectați containerul dorit din fereastra din stânga. Entitățile vor fi afișate în tabelul din partea dreaptă a ecranului.
3. Selectați stația de lucru de pe care doriți să dezinstalați Protecția Exchange.

4. Faceți clic pe **Reconfigurare client** din meniul **Sarcini** din partea superioară a tabelului. Este afișată o fereastră de configurare.
5. În secțiunea **General**, debifați caseta **Exchange Protection**.

**Avertisment**

În fereastra de configurare, asigurați-vă că ați selectat toate celelalte roluri active pe stația de lucru. În caz contrar, acestea vor fi dezinstalate.

6. Faceți clic pe **Salvare** pentru a genera sarcina.

Puteți vizualiza și administra sarcina în **Rețea > Sarcini**.

Dacă doriți să reinstalați Protecția Exchange, consultați „[Instalarea Exchange Protection](#)” (p. 65).

8. OBȚINERE AJUTOR

Bitdefender se străduiește să ofere clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic. Dacă vă confrunțați cu o problemă sau dacă aveți orice întrebare cu privire la produsul Bitdefender dvs., mergeți la [Centrul de asistență online](#). Acesta oferă mai multe resurse pe care le puteți folosi pentru a găsi rapid o soluție sau un răspuns. Sau, dacă preferați, puteți contacta echipa de Servicii clienți a Bitdefender. Reprezentanții noștri pentru suport tehnic vă vor răspunde la întrebări la timp și vă vor oferi asistența de care aveți nevoie.



Notă

Puteți afla informații despre serviciile de suport oferite și politica noastră de suport la Centrul de asistență.

8.1. Centrul de asistență Bitdefender

[Centrul de asistență Bitdefender](#) este locul unde veți găsi tot ajutorul de care aveți nevoie pentru produsul dumneavoastră Bitdefender.

Puteți utiliza mai multe resurse pentru a găsi rapid o soluție sau un răspuns:

- Articolele din Knowledge Base
- Forum asistență Bitdefender
- Documentație de produs

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare privind securitatea calculatoarelor, produsele și compania Bitdefender.

Articolele din Knowledge Base

Bitdefender Knowledge Base este o bază online de informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea virusilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Bitdefender Knowledge Base este deschisă pentru public și putând fi efectuate căutări în mod liber. Prin intermediul informațiilor extinse pe care le conține, putem oferi clienților Bitdefender cunoștințele tehnice și înțelegerea de care au nevoie. Toate solicitările valide pentru informații sau rapoartele de eroare care vin din

partea clienților Bitdefender ajung la Baza de date Bitdefender sub formă de rapoarte de remediere a erorilor, notițe de evitare a erorilor, articole informaționale pentru a completa fișierele de ajutor ale produsului.

Bitdefender Knowledge Base pentru produsele business este disponibilă oricând la adresa <http://www.bitdefender.ro/support/business.html>.

Forum asistență Bitdefender

Forumul de suport al Bitdefender le oferă utilizatorilor Bitdefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții. Puteți posta orice probleme sau întrebări legate de produsul dumneavoastră Bitdefender.

Tehnicienii pentru suport tehnic ai Bitdefender monitorizează forumul pentru a verifica noile postări cu scopul de a vă ajuta. De asemenea, puteți obține un răspuns sau o soluție de la un utilizator Bitdefender cu mai multă experiență.

Înainte de a posta problema sau întrebarea, sunteți rugat să verificați în forum existența unui subiect similar sau corelat.

Forumul de suport al Bitdefender este disponibil la <https://forum.bitdefender.com>, în 5 limbi diferite: engleză, germană, franceză, spaniolă și română. Faceți clic pe link-ul **Protecție Business** pentru a accesa secțiunea dedicată produselor business.

Documentație de produs

Documentația de produs este sursa cea mai completă de informații despre produs. Efectuați clic pe numele de utilizator din colțul din dreapta sus al consolei, selectați **Ajutor & Asistență** și apoi accesați linkul ghidului care vă interesează. Ghidul se va deschide într-un nou tab în browser.

8.2. Solicitarea de asistență profesională

Puteți solicita asistență prin intermediul Centrului nostru de asistență online. Completați [formularul de contact](#) și transmiteți-l.

8.3. Utilizarea Modulului de Suport Tehnic

Modulul de Suport Tehnic GravityZone este conceput pentru a ajuta utilizatorii și pentru a sprijini tehnicienii în obținerea cu ușurință a informațiilor necesare pentru rezolvarea problemelor. Rulați Modululul de Suport Tehnic pe calculatoarele afectate și trimiteți arhiva rezultată cu informațiile de depanare la reprezentantul de asistență al Bitdefender .

8.3.1. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Windows

Se execută Modulul de Suport Tehnic

Pentru a genera jurnalul pe calculatorul afectat, utilizați una din metodele de mai jos:

- **Linia de comandă**
Pentru orice probleme cu BEST, instalat pe computer.
- **Problemă la instalare**
Pentru situațiile în care BEST nu este instalat pe computer și instalarea eșuează.

Metode liniei de comandă

Utilizând linia de comandă, puteți colecta jurnalele direct de la computerul afectat. Această metodă este utilă în situațiile în care nu aveți acces la GravityZone Control Center sau în care computerul nu comunică cu consola.

1. Deschideți Command Prompt cu privilegiile de administrator.
2. Mergeți la folderul de instalare al produsului. Călea implicită este:
C:\Program Files\Bitdefender\Endpoint Security
3. Colectați și salvați jurnalele prin executarea acestei comenzi:

```
Product.Support.Tool.exe collect
```

Jurnalele sunt salvate implicit în C:\Windows\Temp.

Opțional, în cazul în care doriți să salvați jurnalul instrumentului de suport într-o altă locație, utilizați călea opțională:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Exemplu:

```
Product.Support.Tool.exe collect path="D:\Test"
```

În timpul executării comenzii, veți observa o bară de progres pe ecran. Atunci când procesul s-a încheiat, este afișată denumirea arhivei care conține jurnalele și locația acesteia.

Pentru trimiterea jurnalelor către Bitdefender Enterprise Support accesați `C:\Windows\Temp` sau locația personalizată și căutați fișierul de arhivă denumit `ST_[computername]_[currentdate]`. Atașați arhiva la tichetul de asistență pentru remedierea problemelor.

Problemă la instalare

1. Pentru a descărca Instrumentul de suport BEST, faceți clic [aici](#).
2. Rulați fișierul executabil ca administrator. Va apărea o fereastră.
3. Alegeți o locație în care să salvați arhiva jurnalelor.

Pe măsură ce jurnalele sunt colectate, vei observa o bară de progres pe ecran. Atunci când procesul s-a încheiat, este afișată denumirea arhivei și locația acesteia.

Pentru trimiterea jurnalelor către Bitdefender Enterprise Support, accesați locația selectată și căutați fișierul de arhivă `ST_[computername]_[currentdate]`. Atașați arhiva la tichetul de asistență pentru remedierea problemelor.

8.3.2. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Linux

Pentru sistemele de operare Linux, Modulul de Suport Tehnic este integrat cu agentul de securitate Bitdefender.

Pentru a colecta informațiile de sistem Linux folosind Modulul de Suport Tehnic, executați următoarea comandă:

```
# /opt/BitDefender/bin/bdconfigure
```

folosind următoarele opțiuni disponibile:

- `--help` pentru afișarea tuturor comenzilor aferente Modulului de Suport Tehnic
- `enablelogs` pentru activarea jurnalelor modulului produs și de comunicare (toate serviciile vor fi repornite automat)

- `disablelogs` pentru dezactivarea jurnalelor modulului produs și de comunicare (toate serviciile vor fi repornite automat)
- `deliverall` pentru a crea:
 - O arhivă cu jurnalele produsului și ale modulului de comunicare, transmisă către directorul `/tmp` în următorul format:
`bitdefender_machineName_timeStamp.tar.gz`.

După ce arhiva a fost creată:

1. Veți fi întrebat dacă doriți să dezactivați jurnalele. Dacă este necesar, serviciile sunt repornite automat.
 2. Veți fi întrebat dacă doriți să ștergeți jurnalele.
- `deliverall -default` transmite aceleași informații ca și opțiunea anterioară, însă se iau acțiuni implicite asupra jurnalelor, fără ca utilizatorul să fie întrebat (jurnalele sunt dezactivate și șterse).

De asemenea, puteți executa comanda `/bdconfigure` direct din pachetul BEST (kitul complet sau aplicația de descărcare) fără ca produsul să fie instalat.

Pentru a raporta o problemă GravityZone care vă afectează sistemele Linux, urmați pașii de mai jos, folosind opțiunile descrise anterior:

1. Activați jurnalele pentru produs și modulul de comunicare.
2. Încercați să reproduceți problema.
3. Dezactivați jurnalele.
4. Creați arhiva jurnalelor.
5. Deschideți un bilet de asistență prin e-mail folosind formularul disponibil pe pagina de **Support tehnic** din Control Center, cu o descriere a problemei și jurnalele atașate.

Modulul de Suport Tehnic pentru Linux furnizează următoarele informații:

- Directoarele etc, `var/log`, `/var/crash` (dacă este disponibil) și `var/epag` din `/opt/BitDefender`, cu jurnalele și setările Bitdefender
- Fișierul `/var/log/BitDefender/bdinstall.log`, care conține informații referitoare la instalare

- Fișierul `network.txt`, care conține informații privind setările de rețea/ conectivitatea mașinii
- Fișierul `product.txt`, care include conținutul tuturor fișierelor `update.txt` din `/opt/BitDefender/var/lib/scan` și o listă recursivă completă a tuturor fișierelor din `/opt/BitDefender`
- Fișierul `system.txt`, care conține informații generale despre sistem (versiune distribuție și kernel, memorie RAM disponibilă și spațiul liber pe hard-disk)
- Fișierul `users.txt`, care conține informații referitoare la utilizator
- Alte informații privind produsul asociat sistemului, cum ar fi conexiunile externe ale proceselor și utilizarea CPU
- Jurnale de sistem

8.3.3. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Mac

La trimiterea unei solicitări către echipa de suport tehnic a Bitdefender, este necesar să furnizați următoarele:

- O descriere detaliată a problemei întâmpinate.
- O captură de ecran (dacă este cazul) care să includă exact mesajul de eroare afișat.
- Jurnalul Modulului de Suport Tehnic.

Pentru a colecta informații despre sistemul Mac folosind Modulul de Suport Tehnic:

1. Descărcați [arhiva ZIP](#) conținând Modulul de Suport Tehnic.
2. Extrageți fișierul **BDProfiler.tool** din arhivă.
3. Deschideți o fereastră Terminal.
4. Navigați la locația fișierului **BDProfiler.tool**.

De exemplu:

```
cd /Users/Bitdefender/Desktop;
```

5. Adăugați drepturi de executare pentru fișierul:

```
chmod +x BDProfiler.tool;
```

6. Executați modulul.

De exemplu:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Apăsați D și introduceți parola atunci când vi se solicită să furnizați parola de administrator.

Așteptați câteva minute până când modulul finalizează generarea jurnalului. Veți găsi fișierul de arhivă rezultat (**Bitdefenderprofile_output.zip**) pe desktop.

8.4. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 18 ani Bitdefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

8.4.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro

Centrul de asistență: <http://www.bitdefender.ro/support/business.html>

Documentație: gravityzone-docs@bitdefender.com

Distribuitori locali: <http://www.bitdefender.ro/partners>

Programe de Parteneriat: partners@bitdefender.com

Relații Media: pr@bitdefender.com

Subscrieri viruși: virus_submission@bitdefender.com

Subscrieri spam: spam_submission@bitdefender.com

Raportare abuz: abuse@bitdefender.com

Website: <http://www.bitdefender.com>

8.4.2. Distribuitori locali

Distribuitorii locali Bitdefender sunt pregătiți să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergeți la <http://www.bitdefender.ro/partners>.
2. Mergeți la **Localizare partener**.
3. Datele de contact ale distribuitorilor locali Bitdefender ar trebui să se afișeze automat. În caz contrar, selectați țara de reședință pentru a accesa aceste informații.
4. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa enterprisesales@bitdefender.com.

8.4.3. Filialele Bitdefender

Reprezentanțele Bitdefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

Statele Unite ale Americii

Bitdefender, LLC

PO Box 667588

Pompano Beach, FL 33066

United States

Telefon (vânzări&suport tehnic): 1-954-776-6262

Vânzări: sales@bitdefender.com

Web: <http://www.bitdefender.com>

Centrul de asistență: <http://www.bitdefender.com/support/business.html>

Franța

Bitdefender

49, Rue de la Vanne

92120 Montrouge

Fax: +33 (0)1 47 35 07 09

Telefon: +33 (0)1 47 35 72 73

E-mail: b2b@bitdefender.fr

Site-ul web: <http://www.bitdefender.fr>

Centrul de asistență: <http://www.bitdefender.fr/support/business.html>

Spania

Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª

08037 Barcelona

España

Fax: (+34) 93 217 91 28

Telefon (birou&vânzări): (+34) 93 218 96 15

Telefon (suport tehnic): (+34) 93 502 69 10

Vânzări: comercial@bitdefender.es

Site-ul web: <http://www.bitdefender.es>

Centrul de asistență: <http://www.bitdefender.es/support/business.html>

Germania

Bitdefender GmbH

Technologiezentrum Schwerte

Lohbachstrasse 12

D-58239 Schwerte

Deutschland

Telefon (birou&vânzări): +49 (0) 2304 94 51 60

Telefon (suport tehnic): +49 (0) 2304 99 93 004

Vânzări: firmenkunden@bitdefender.de

Site-ul web: <http://www.bitdefender.de>

Centrul de asistență: <http://www.bitdefender.de/support/business.html>

Marea Britanie și Irlanda

Genesis Centre Innovation Way

Stoke-on-Trent, Staffordshire

ST6 4BF

UK

Telefon (vânzări&suport tehnic): (+44) 203 695 3415

E-mail: info@bitdefender.co.uk

Vânzări: sales@bitdefender.co.uk

Site-ul web: <http://www.bitdefender.co.uk>

Centrul de asistență: <http://www.bitdefender.co.uk/support/business.html>

România

BITDEFENDER SRL

Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Telefon (vânzări&suport tehnic): +40 21 2063470
Vânzări: sales@bitdefender.ro
Site-ul web: <http://www.bitdefender.ro>
Centrul de asistență: <http://www.bitdefender.ro/support/business.html>

Emiratele Arabe Unite

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (vânzări&suport tehnic): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vânzări: sales@bitdefender.com
Web: <http://www.bitdefender.com>
Centrul de asistență: <http://www.bitdefender.com/support/business.html>

A. Anexe

A.1. Tipuri de fișiere acceptate

Motoarele de scanare antimalware incluse în soluțiile de securitate Bitdefender pot scana toate tipurile de fișiere care ar putea conține amenințări. Lista de mai jos cuprinde cele mai des întâlnite tipuri de fișiere care sunt analizate.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo

A.2. Obiecte Sandbox Analyzer

A.2.1. Tipuri și extensii de fișiere acceptate pentru trimitere manuală

Următoarele extensii de fișiere sunt acceptate și pot fi detonate manual în Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, fișiere MZ/PE (executabile), PDF, PEF (executabile), PIF (executabile), RTF, SCR, URL (binar), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer poate detecta tipurile de fișiere menționate mai sus și dacă sunt include în arhive de următoarele tipuri: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, Arhivă comprimată LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolum), ZOO, XZ.

A.2.2. Tipurile de fișiere acceptate de modulul de filtrare preliminară a conținutului la trimiterea automată

Filtrarea preliminară a conținutului va stabili un anumit tip de fișier prin intermediul unei combinații care include conținutul și extensia obiectului. Acest lucru înseamnă că un fișier executabil cu extensia .tmp va fi recunoscut ca fiind o aplicație și, dacă este depistat ca fiind suspect, va fi trimis către Sandbox Analyzer.

- Aplicații - fișiere care au formatul PE32, inclusiv, dar fără a se limita la următoarele extensii: exe, dll, com.
- Documente - fișiere cu format de document, inclusiv, dar fără a se limita la următoarele extensii: xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf.

- Script-uri: ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.
- Arhive: zip, jar, 7z, bz, bz2, tgz, msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.
- E-mail-uri (memorate în sistemul de fișiere): eml, tnef.

A.2.3. Excluderi implicite la trimiterea automată

asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.

A.3. Kerneluri compatibile cu senzorul de incidente

Senzorul de incidente este compatibil cu următoarele kerneluri: