Bitdefender GravityZone

Il modulo Antimalware

7 Giugno 2018

Roberto Novasconi

Avangate Italia - Senior Support and Training Specialist

Bitdefender
AUTHORIZED DISTRIBUTOR

AVANGATE
Distributore a valore aggiunto

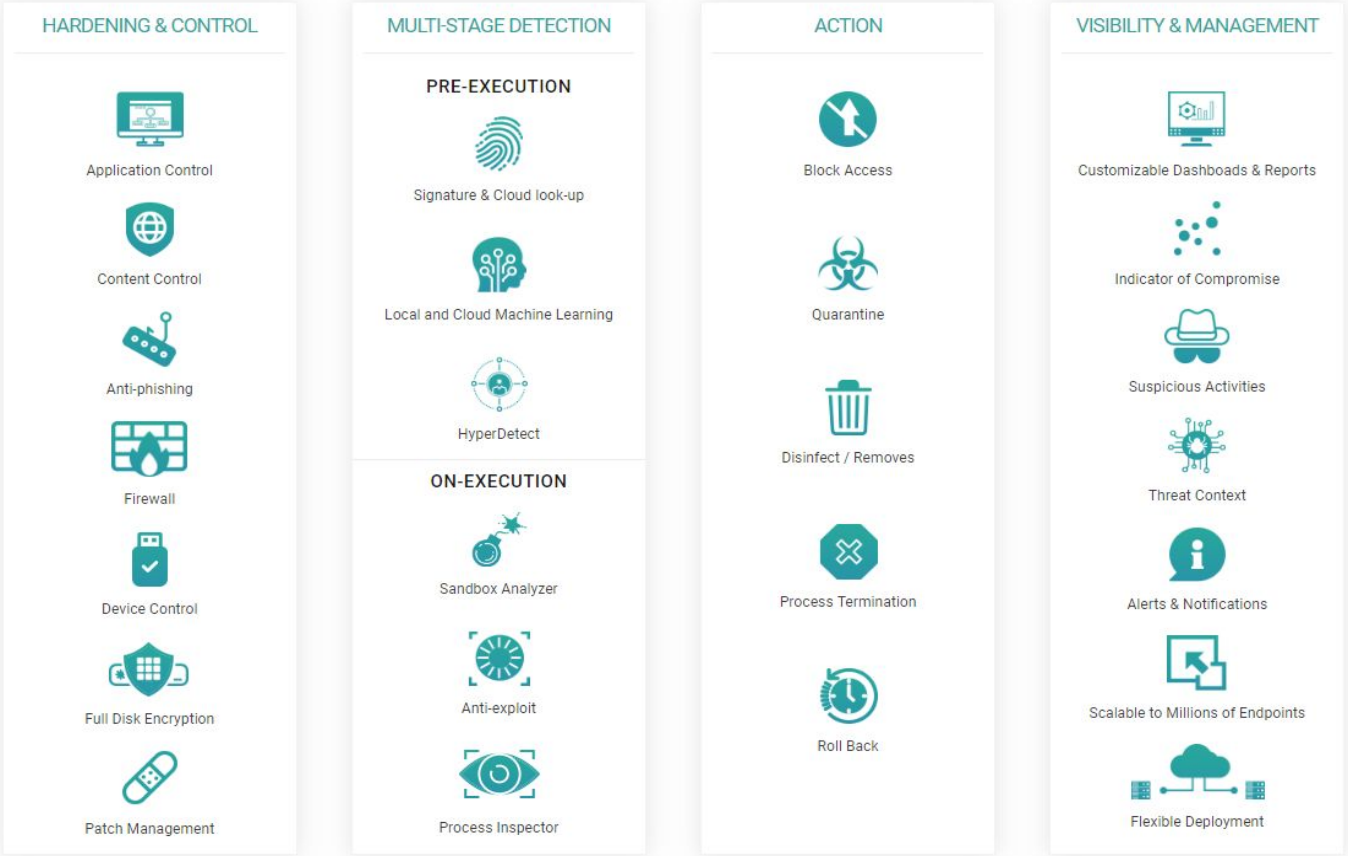
GravityZone

Agenda

- **PRESENTAZIONE**
  Conoscere i dispositivi antimalware
- **DEMO**
  reportistica, eccezioni, best practice
- **RISORSE E CONTATTI**
- **SPAZIO PER LE VS DOMANDE**

AVANGATE
Distributore a valore aggiunto

BEST - Bitdefender Enpoint Security Tools



https://www.bitdefender.com/business/elite-security.html

BEST - Antimalware

MULTI-STAGE DETECTION

PRE-EXECUTION

Signature & Cloud look-up

Local and Cloud Machine Learning

ON-EXECUTION

Anti-exploit

Process Inspector

ACTION

Block Access

Quarantine

Disinfect / Removes

Process Termination

Roll Back

GravityZone

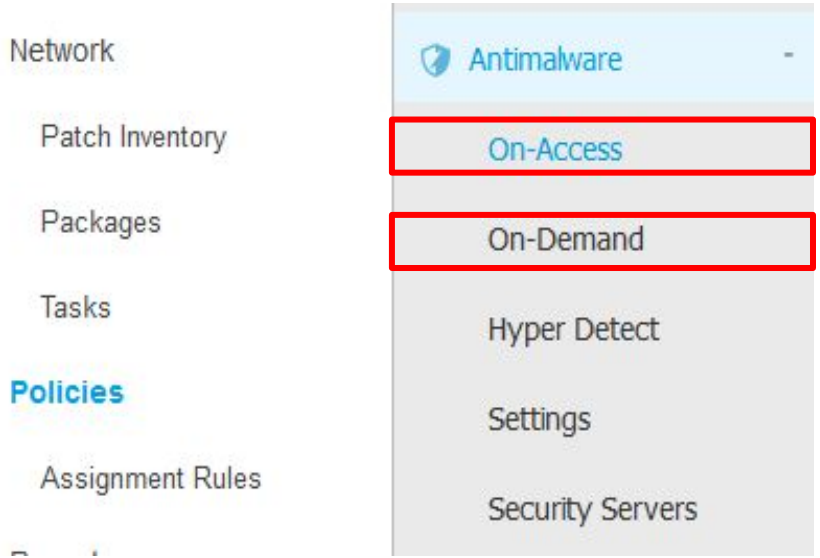
Modulo Antimalware - dove e quando

- si installa su **tutte le piattaforme** supportate da GravityZone
- si attiva con **TUTTE le licenze** GravityZone
- è **obbligatorio** in TUTTE le installazioni GravityZone

AVANGATE
Distributore a valore aggiunto

GravityZone

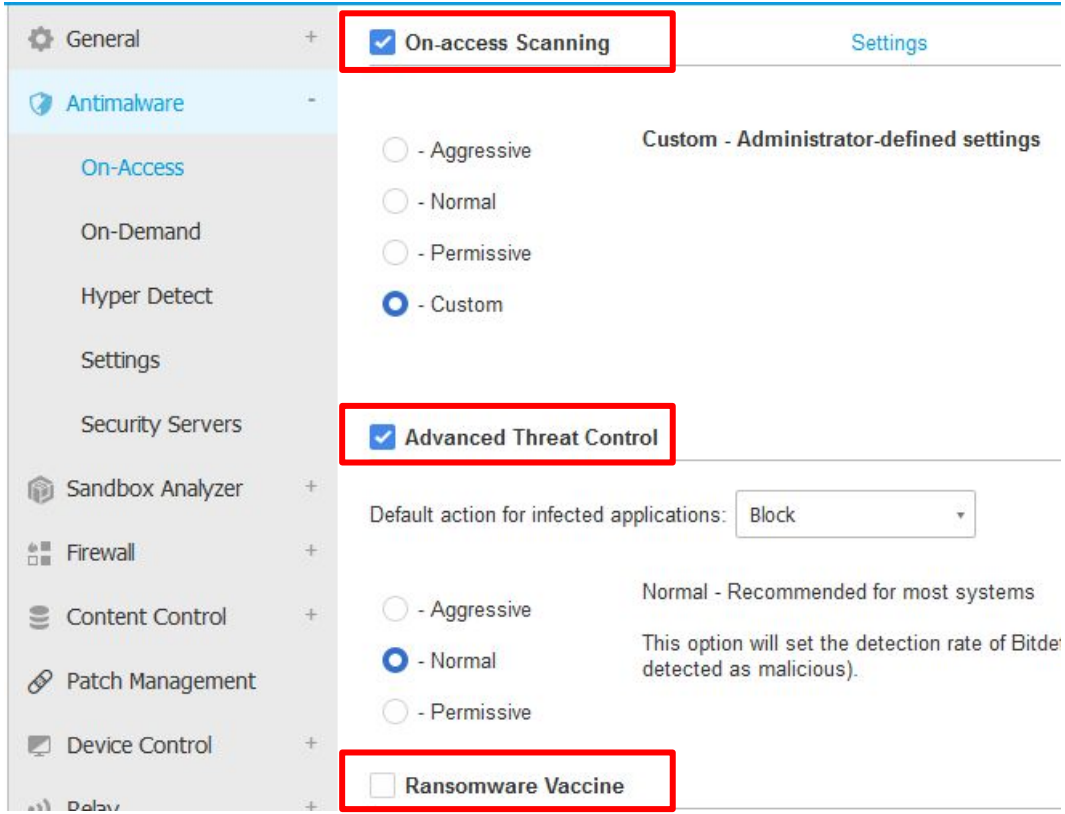
Modulo Antimalware - Policy



AVANGATE
Distributore a valore aggiunto

GravityZone

Antimalware → **OnAccess**



AVANGATE
Distributore a valore aggiunto

GravityZone

Antimalware → OnAccess → **On-access Scanning**

- scansione dei file all'accesso
- opera in **pre-execution**
- signature based + BeHavioral analisys (B-Have)
- è disponibile per tutte le piattaforme

AVANGATE
Distributore a valore aggiunto

GravityZone

Antimalware → OnAccess → Advanced Threat Control **ATC**

- controllo comportamentale dei processi
- opera **on-execution**
- ignora la natura del file, ne verifica esclusivamente il comportamento*
- interviene all'apertura del file, ma solo se e quando rileva comportamenti sospetti
- è disponibile solo per Windows**
- **è determinante ai fini della protezione AntiExpolit e AntiRansomware**
- **rispetta esclusivamente le eccezioni di tipo Process**

AVANGATE
Distributore a valore aggiunto

GravityZone

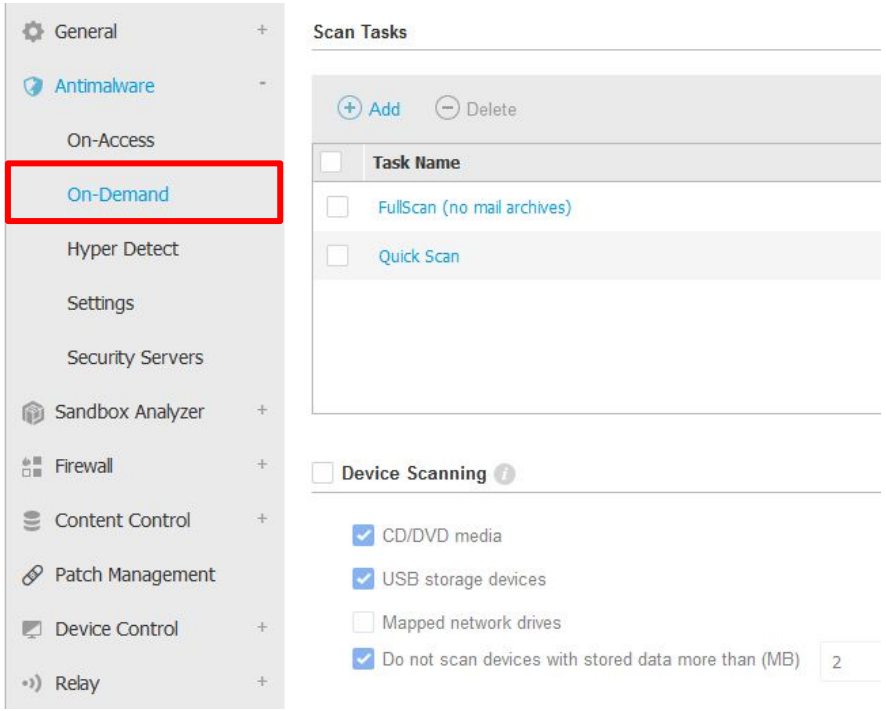
Antimalware → OnAccess → **Ransomware Vaccine**

- inserisce in Windows i marker tipici delle famiglie note di attacchi ransomware
- in presenza dei marker, queste famiglie di attacchi NON effettuano la cifratura
- ha effetto solo su Windows
- NON comporta alcuna incompatibilità o impatto sulle performances; lo attiviamo sempre
- **NON rappresenta l'elemento chiave ai fini della protezione AntiRansomware (ATC lo è)**

AVANGATE
Distributore a valore aggiunto

GravityZone

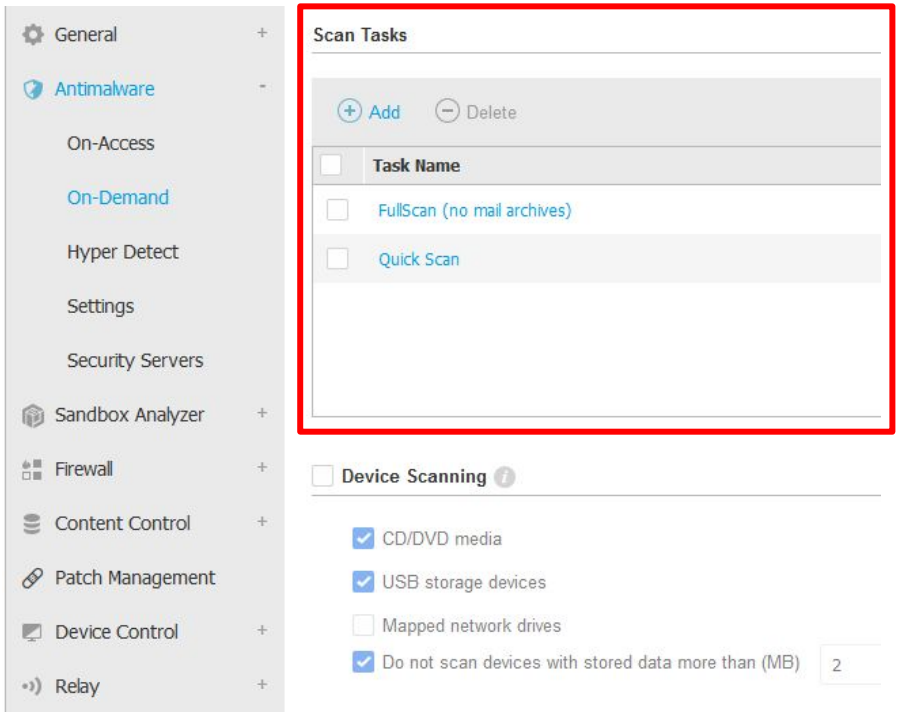
Antimalware → **OnDemand**



AVANGATE
Distributore a valore aggiunto

GravityZone

Antimalware → **OnDemand** → **Scan Tasks**

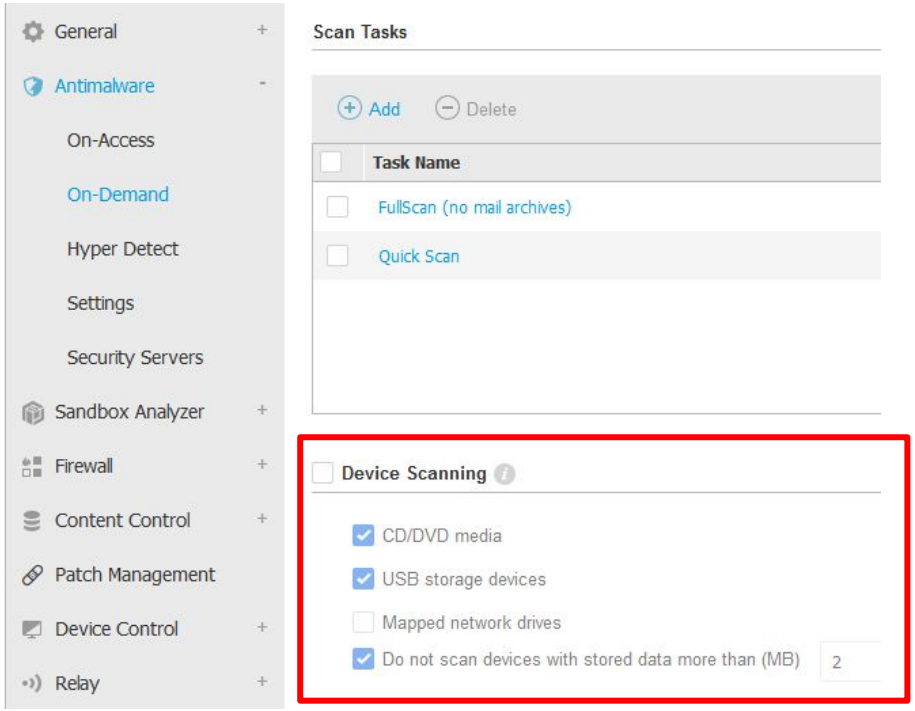


*Permette di **pianificare** scansioni di memoria, filesystem, e registry.*

AVANGATE
Distributore a valore aggiunto

GravityZone

Antimalware → **OnDemand** → **Device Scanning**



Scansiona
***l'intero contenuto** dei supporti rimovibili ,*
***al loro inserimento/collegamento**.*

Attivare con cautela !

AVANGATE
Distributore a valore aggiunto

GravityZone

Antimalware - **OnDemand**

- permette di censire il contenuto dei supporti
- non interviene nell'avvio dei programmi
- può avviare attività molto lunghe ed impattanti sulle performances
- se utilizzato con frequenza eccessiva può stressare i supporti dispositivi
- **NON aumenta la protezione dell'enpoint**

AVANGATE
Distributore a valore aggiunto

GravityZone

Demo

- usare la dashboard
- usare i report
- usare le notifiche
- definire esclusioni per ATC
- definire esclusioni per OnAccess Scanner
- disattivare temporaneamente la protezione
  https://supporto.avangate.it/kb/knowledgebase.php?article=288

AVANGATE
Distributore a valore aggiunto

Bitdefender

risorse e contatti

Bitdefender Training Center
(*chiedere l'account ad Avangate Italia*)
http://elearning.bitdefender.com/bitdefender/

Bitdefender Enterprise in YouTube
https://www.youtube.com/user/BitdefenderSecurity/videos

Bitdefender Centro Supporto Business (Knoweldgebase, Ticket, Chat)
https://www.bitdefender.com/support/business/

Bitdefender GravityZone Guide Utente e richiesta supporto
In console, Wellcome, [username]/Help & Support

AVANGATE
Distributore a valore aggiunto

Avangate Italia

risorse e contatti

Primo contatto

www.avangate.it/contattaci

sales@avangate.it

02 89607318

Diventa Partner Avangate Italia

http://www.avangate.it

Rivenditori → Diventa Rivenditore

Portale Supporto Avangate Italia (KB, Chat, Ticket)

http://supporto.avangate.it

AVANGATE

Distributore a valore aggiunto

Domande

Utilizzare la sezione Domande del pannello GoToMeeting

AVANGATE
Distributore a valore aggiunto

AVANGATE

Distributore a valore aggiunto

Bitdefender
AUTHORIZED DISTRIBUTOR

Alexandru Stefan
Bitdefender Product Manager

Roberto Novasconi
Senior Tech Support and Training Specialist

GRAZIE