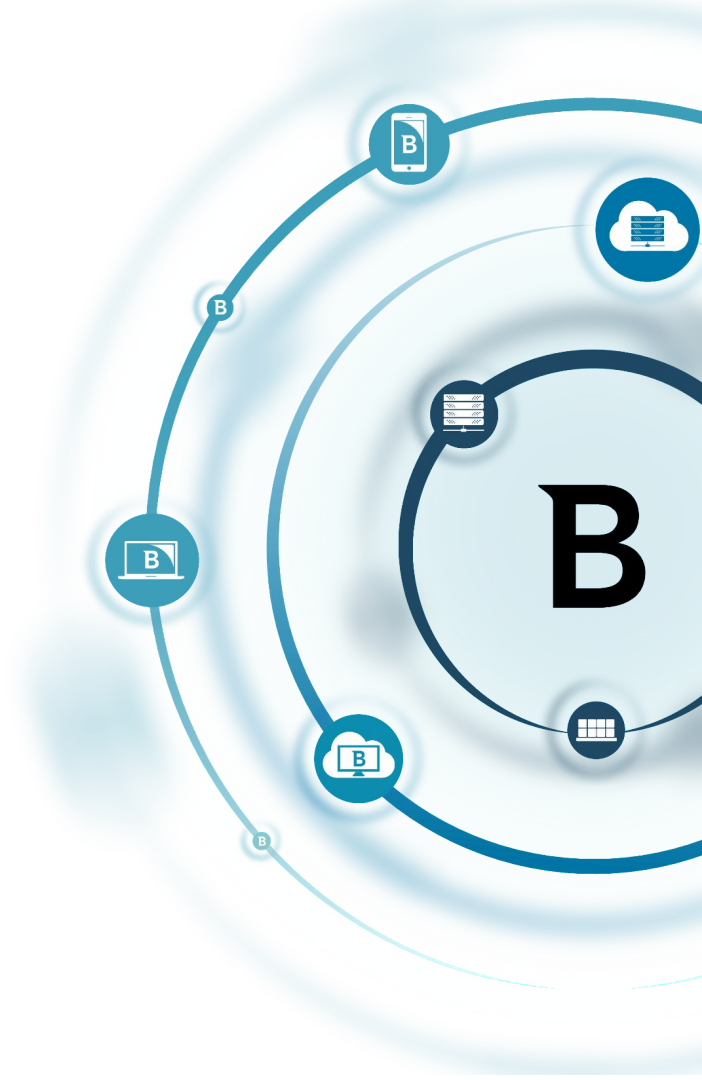


Procedura per il Partner

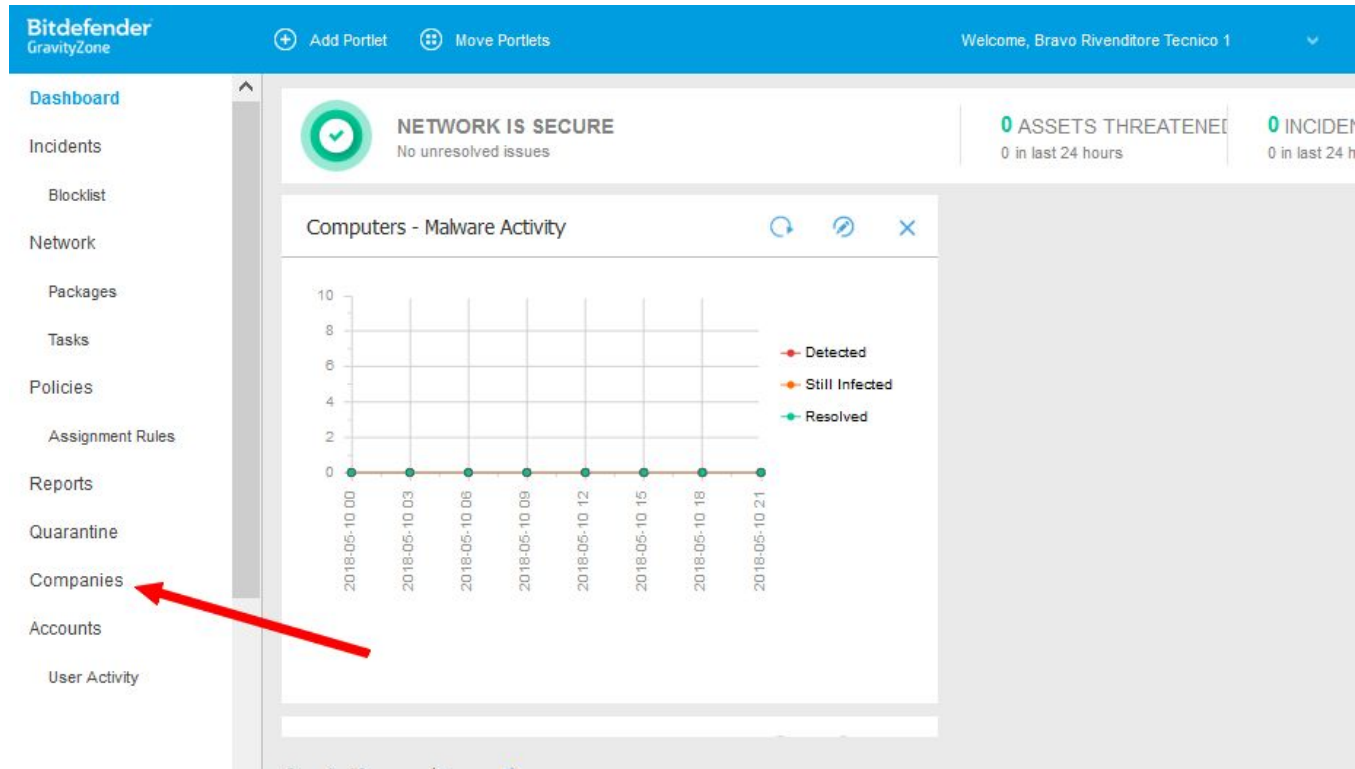
BITDEFENDER GRAVITYZONE

Attivare Full Disk Encryption per il cliente



Accedo a GravityZone Cloud console come partner:

<https://gravityzone.bitdefender.com>



Dashboard

Incidents

Blocklist

Network

Packages

Tasks

Policies

Assignment Rules

Reports

Quarantine

Companies

Accounts

User Activity

 Add  Activate  Suspend  Delete  Refresh

	Name	Type	Managed	License usage
☐				
☐	 Bravo Cliente	Customer	Yes	Licensed: 0, Unl
☐	 Bravo Cliente 2	Customer	Yes	Licensed: 0, Tot
☐	 Bravo Cliente3	Customer	Yes	Licensed: 0, Unl



Edit company ✕

Company Details

Company Name:

Address:

My Company ID: 6c916b4f4c542ccb3cf92f7542fe77bd

Phone:

Logo: 
The logo needs to have the size 200px x 30px, and needs to be in .png or .jpg format.

Type:

☒ Manage Networks

License

Type:

Reserve seats:

Expiry date: 19 December 2021

Mailboxes:

Monthly License Usage: 

☐ Allow company to manage Exchange

☒ Allow company to manage Encryption

☐ Allow company to manage Central Scan

☐ Link this company to MyBitdefender (optional)

**Se ho attivato il cliente con
Monthly Subscription (licensing MSP)**

Mi accerto che la company del cliente si
attivata con Monthly Subscription e sia
abilitata al servizio Encryption.

Edit company ×

My Company ID: 7a29a76541bc440d488518ffc480fa62

Phone:

Logo: 
The logo needs to have the size 200px x 30px, and needs to be in .png or .jpg format.

Type:

☒ Manage Networks

Two-factor authentication

Enforce two-factor authentication: ? ☐

License

Type:

License Key:

Expiry date:	Licensed:	Not licensed:	Total:	Available for servers:
20 July 2018	0	0	5	2

Add-on key:

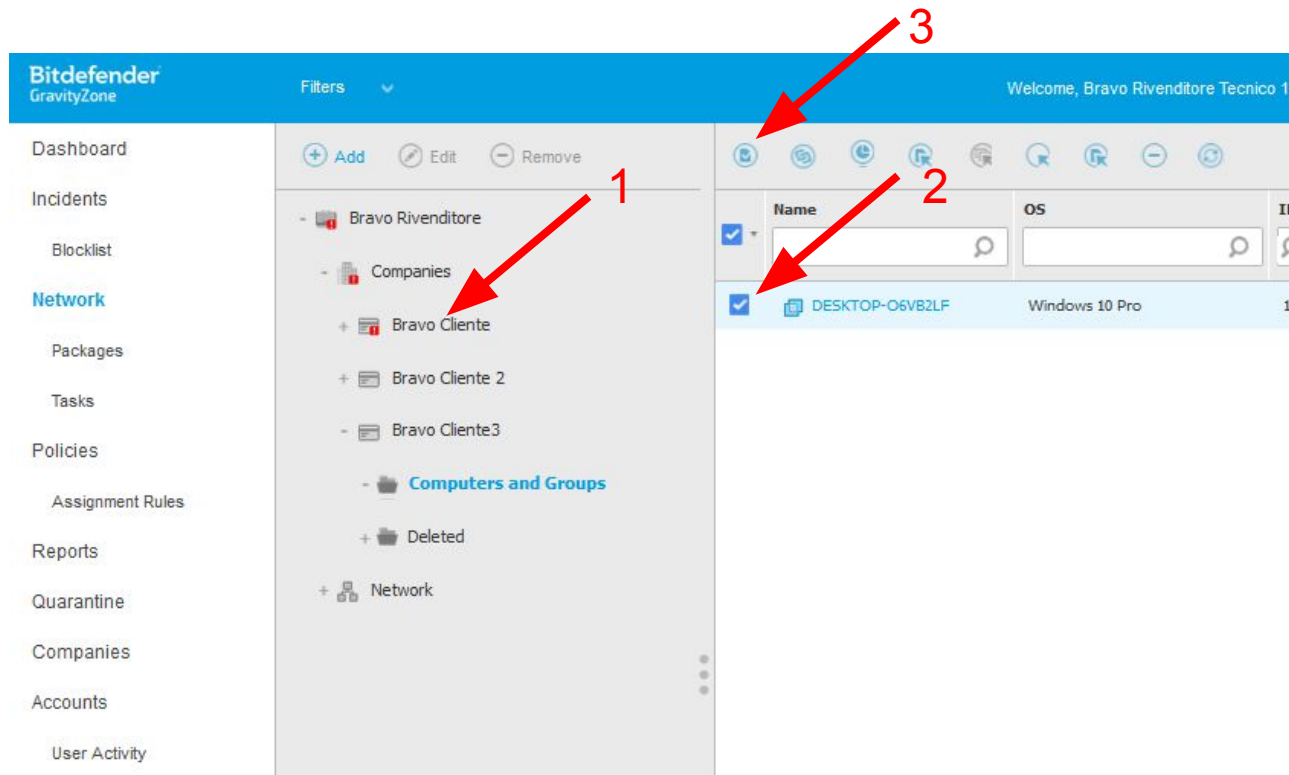
Type:	Key:	Remove:
Encryption	7ZCGQ7R	X

☐ Link this company to MyBitdefender (optional)

Se ho attivato il cliente con licenza Prepagata o TRIAL

1. Nel campo “Add-On key”,
inserisco la chiave add-on
(TRIAL o Prepagata) per Encryption
2. clicco su <Add>
*Se valida, la chiave è aggiunta
immediatamente sotto.*
3. Confermo con <Save> in calce.

Aggiungo il modulo Encryption, su Endpoint già protetti da BEST.
Seleziono gli endpoint compatibili su cui intendo installare il modulo Encryption.



Seleziono gli endpoint compatibili, su cui installare il modulo Encryption.

Per i requisiti, consultare Installation Guide, paragrafo **2.3. Full Disk Encryption Requirements**

Dashboard

Incidents

Blocklist

Network

Packages

Tasks

Policies

Assignment Rules

Reports

Quarantine

Companies

Accounts

User Activity

+ Add Edit - Remove

- Bravo Rivenditore

- Companies

+ Bravo Cliente

+ Bravo Cliente 2

- Bravo Cliente3

- Computers and Groups

+ Deleted

+ Network

Icons for various actions: Scan, Exchange Scan, Install, Upgrade client, Uninstall client, Update client, Reconfigure Client, Restart machine, Network Discovery, Update Security Server

Scan

Exchange Scan

Install

Upgrade client

Uninstall client

Update client

Reconfigure Client

Reconfigure Client

Restart machine

Network Discovery

Update Security Server

OS

IP

LF

Windows 10 Pro

192...

Configuro il task Reconfigure Client, per includere il modulo Encryption, poi lo assegno con <Save>.

ATTENZIONE

I moduli NON contrassegnati, verranno disinstallati, qual'ora presenti. Vanno quindi contrassegnati TUTTI i moduli che si desidera siano presenti sugli endpoint a cui è destinato il task.

Verifico lo stato di il completamento del task.

Bitdefender GravityZone

Welcome, Bravo Rivenditore Tecnico 1

Dashboard

Incidents

Blocklist

Network

Packages

Tasks

Policies

Assignment Rules

Restart Delete Refresh

	Name	Task type	Status	Start period	Company
☐					
☐	Reconfigure client settings 2018-05-10	Reconfigure client	Finished (1 / 1)	10 May 2018, 16:00:46	Bravo Cliente3

1

2

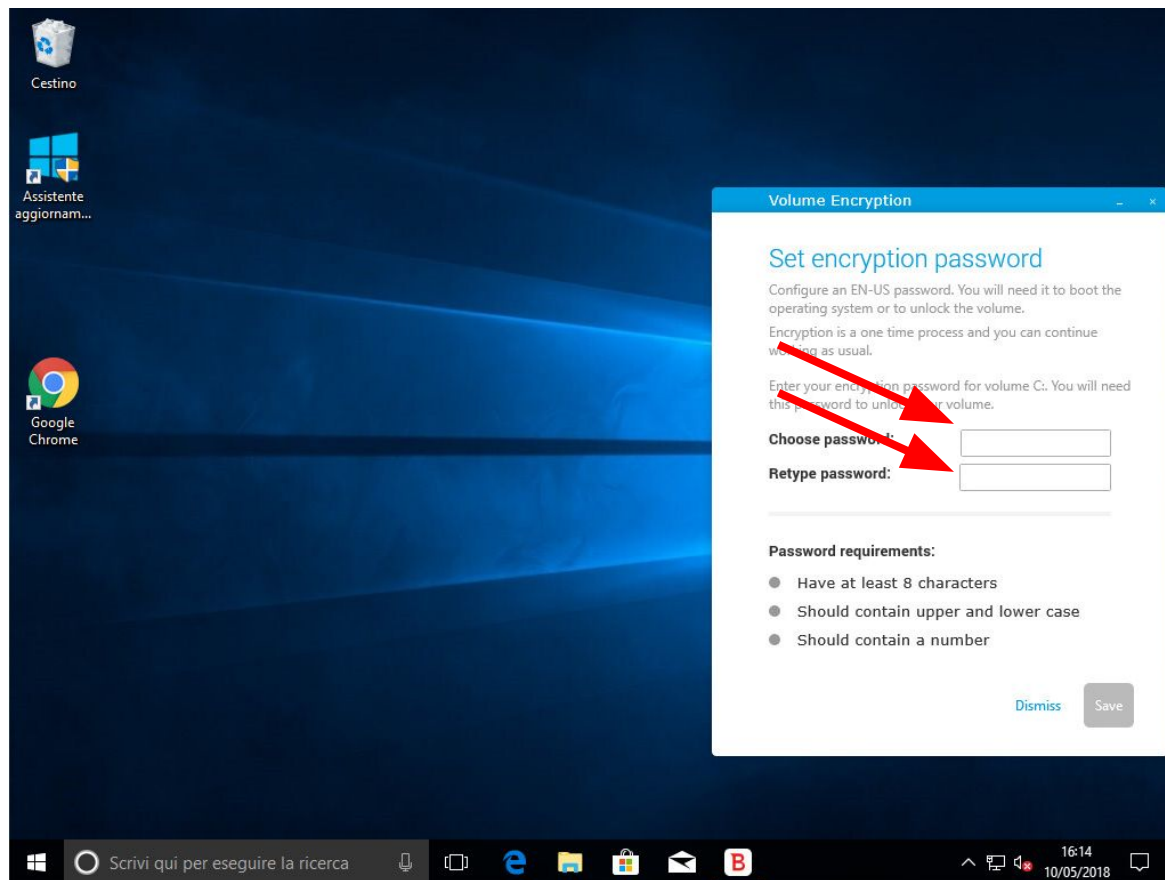
Per attivare l'encryption, edito la policy applicata agli endpoint interessati

The screenshot shows the Bitdefender GravityZone web interface. The left sidebar contains a navigation menu with items like Dashboard, Incidents, Blocklist, Network, Packages, Tasks, Policies, Assignment Rules, Reports, Quarantine, Companies, Accounts, and User Activity. The 'Network' section is expanded, showing a tree view with 'Bravo Rivenditore', 'Companies', 'Bravo Cliente', 'Bravo Cliente 2', 'Bravo Cliente3', 'Computers and Groups', and 'Deleted'. The 'Computers and Groups' item is selected. The main area displays a table of endpoints. The table has columns: Name, OS, IP, Last Seen, Label, Policy, and Company. The first row shows 'DESKTOP-O6VB2LF', 'Windows 10 Pro', '192.16...', 'Now', 'N/A', 'Default Policy for Cliente3', and 'Bravo Cliente3'. A red arrow labeled '1' points to the 'Network' menu item. A red arrow labeled '2' points to the 'Computers and Groups' item. A red arrow labeled '3' points to the 'Policy' dropdown menu in the table header.

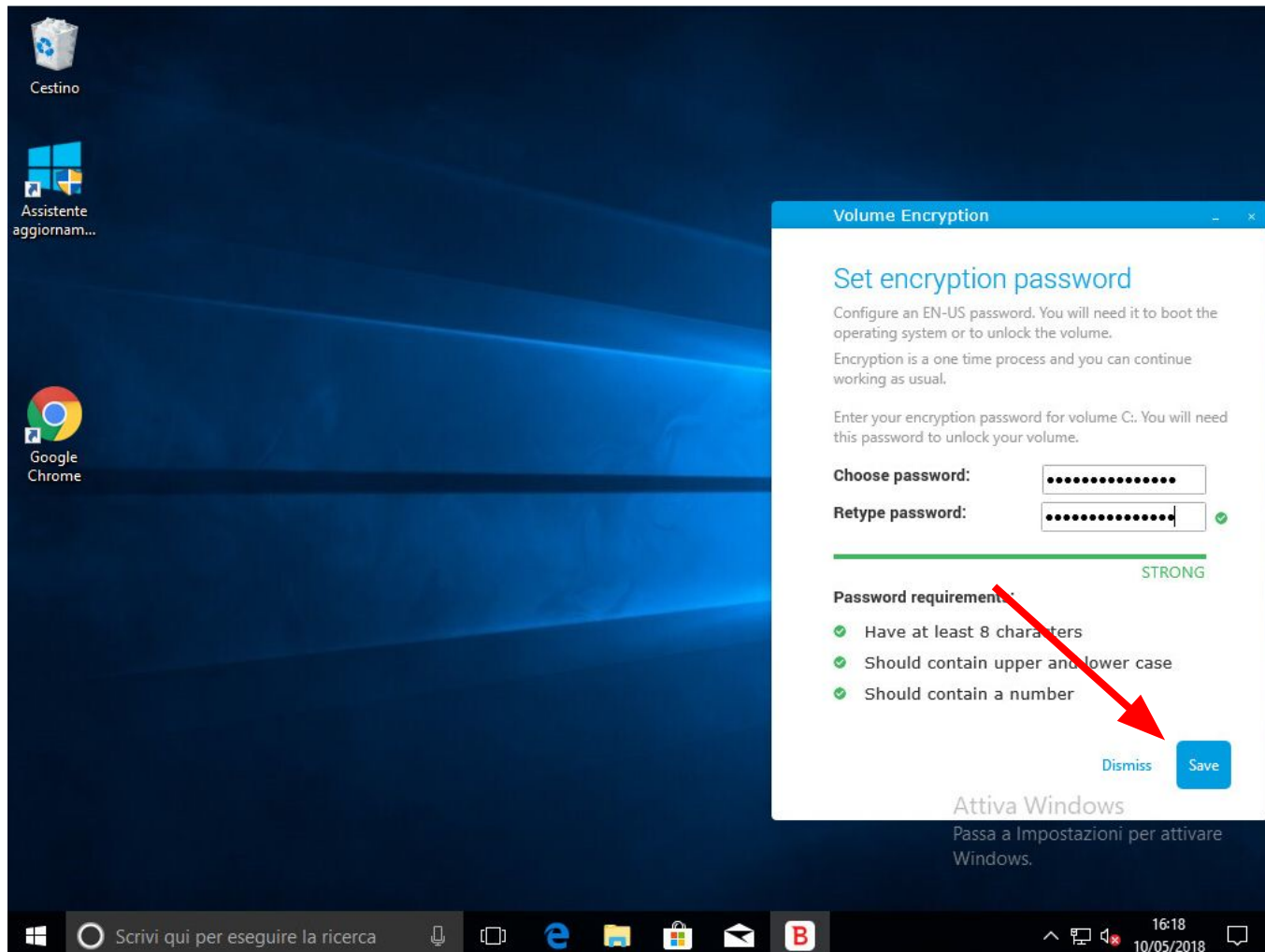
The screenshot displays the Bitdefender GravityZone interface. The top navigation bar is blue with the Bitdefender GravityZone logo on the left and a welcome message 'Welcome, Bravo Rivenditore Tecnico 1' on the right. A left sidebar lists various management sections: Dashboard, Incidents, Blocklist, Network, Packages, Tasks, Policies (highlighted in blue), Assignment Rules, Reports, Quarantine, Companies, Accounts, and User Activity. The 'Policies' section is expanded, showing a list of policy categories: General, Antimalware, Sandbox Analyzer, Firewall, Content Control, Device Control, Relay, Exchange Protection, Encryption (highlighted in blue), and EDR Sensor. The 'Encryption' policy is selected, showing its configuration. At the top of the configuration pane, the 'Encryption Management' checkbox is checked. Below it, a description states: 'Enable this module to start managing endpoint encryption from Control Center. Disabling it will leave volumes in their current state and will allow users to manage encryption locally.' Two radio buttons are present: 'Decrypt' (unselected) and 'Encrypt' (selected). The 'Encrypt' option has a description: 'Select this option to encrypt volumes. Users will be prompted to enter a password that will be required for pre-boot authentication.' Below the radio buttons, there is a checkbox labeled 'If Trusted Platform Module (TPM) is active, no to ask for pre-boot password.' which is currently unchecked. Three red arrows are overlaid on the image: one points to the 'Encryption Management' checkbox, another points to the 'Encrypt' radio button, and a third points to the 'Encryption' menu item in the left sidebar.

Nella policy, attivo il modulo Encryption e l'opzione "Encrypt".

La variazione ha effetto immediato su tutti gli endpoint che hanno applicata tale policy ed hanno installato il modulo Encryption.

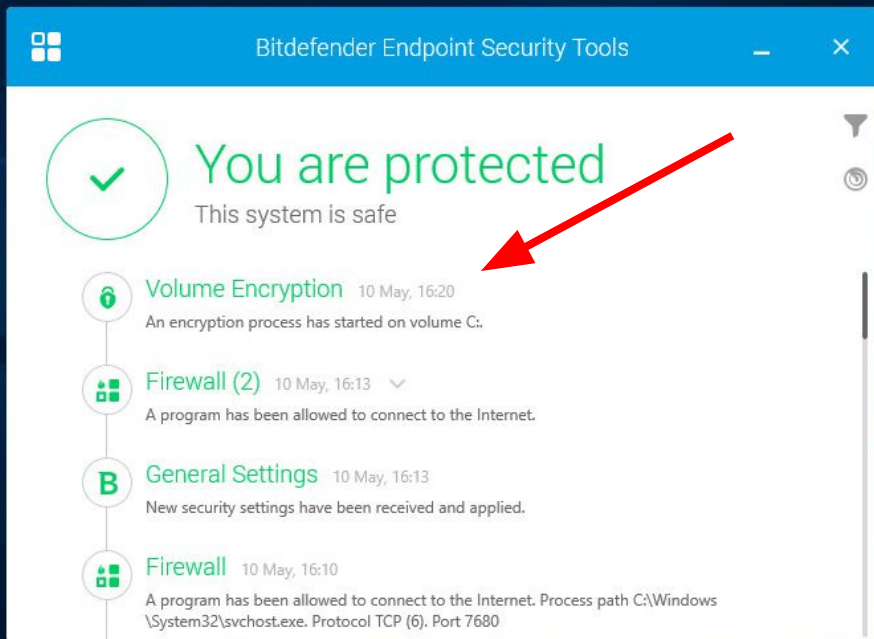


Non appena l'enpoint applica la variazione della policy, l'utente del computer ha visualizzato il popup di Bitdefender, che lo invita a specificare la password per la cifratura dei volumi.



Non appena l'utente conferma, con click su <Save> la password scelta, la cifratura dei volumi ha inizio.

Se l'utente ignora la richiesta, il popup apparirà di nuovo successivamente, fino a quando non verrà fornita una password e conferma per la cifratura.



La restricted GUI sul endpoint ,
fornisce indicazioni in tempo
reale sugli eventi ed attività.

L'inizio della attività di cifratura
dei volumi viene quindi
notificato.

Attiva Windows
Passa a Impostazioni per attivare
Windows.

AVANGATE
Distributore a valore aggiunto

Information

GeneralProtectionPolicyScan Logs

Last signatures update:10 May 2018 16:03:49

Primary scan engine:Central Scan

Fallback scan engine:Hybrid Scan

Overview

Modules

Antimalware:On

Firewall:On

Content Control:On

Power user:Off

Device control:Off

Advanced Threat Control:On

Encryption:On

Reporting(today)

Malware Status:
-> No detections

Malware Activity:
-> No activity

Additional Information

Encryption

C: (boot volume)Encryption in progress (Recovery)

SaveClose

In console,
i dettagli dell'endpoint,
alla voce Protection,
riportano lo stato corrente
della cifratura dei volumi.

AVANGATE
Distributore a valore aggiunto

Bitdefender GravityZone

Welcome, Bravo Rivenditore Tecnico 1

Filters

Dashboard

Incidents

Blocklist

Network

Packages

Tasks

Policies

Assignment Rules

Reports

Quarantine

Companies

Accounts

User Activity

+ Add Edit Remove

- Bravo Rivenditore

- Companies

+ Bravo Cliente

+ Bravo Cliente 2

+ Bravo Cliente3

+ Network

Name OS IP

Bravo Cliente3

Bravo Cliente 2

Bravo Cliente

Posso selezionare la company di cui desidero il report, e cliccare sull'icona Report.

Edit Report

Details

Type: Endpoint Encryption Status

Name: * Endpoint Encryption Status Report

Settings

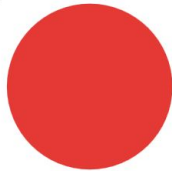
☒ Now
☐ Scheduled

Delivery: ☐ Send by email to

Generate Cancel

Endpoint Encryption Status Report

Generated by: roberto.novasoni-bravori@gmail.com
On: 10 May 2018, 17:09:53
Recurrence: Now
Targets: Bravo Cliente3



Non-compliant with encryption settings

Endpoint Name	Endpoint PQDR	IP	Operating System	Device Policy Com...	Volumes Summary	Device Policy	Company Name
DESKTOP-OVB2LUF	desktop-ovb2luf	192.168.101.56	Windows 10 Pro	Non-compliant	0 / 1	Default Policy for Clien...	Bravo Cliente3

First Page Page 1 of 1 Last Page 20 1 Item

Export Email

Generando un Report di tipo “Enpoint Encryption Status” ottengo informazioni sullo stato di cifratura degli enpoint.

Come ogni report GravityZone, può essere salvato in formato pdf/csv, può essere inviato per email, può essere generato on demand, può essere pianificato.