Deploy - How to

Versione	Data	Redattore	Descrizione
0.9	25/07/2025	Davide Marin	Aggiunto paragrafo “Custom Exclusion Rules”, ritocchi al contenuto
0.8	22/07/2025	Davide Marin	Aggiunto paragrafo “Threats Explorer”, ritocchi al contenuto
0.7	21/07/2025	Davide Marin	Modifiche e migliorie al documento
0.6	18/07/2025	Davide Marin	Continuo stesura capitoli vecchi, aggiunto Risk Management“ e “Gestione dei Report”
0.5	17/07/2025	Davide Marin	Continuo stesura capitoli su politiche, tag, report e “Altre Funzionalità”
0.4	16/07/2025	Davide Marin	Continuo stesura capitoli su politiche e “Altre Funzionalità”
0.3	14/07/2025	Davide Marin	Aggiunto e iniziato a redigere capitolo “Guida alla creazione delle politiche di protezione”
0.2	27/06/2025	Davide Marin	Stesura sezioni “Installare Security Server” e “Guida all’integrazione di Active Directory”
0.1	26/06/2025	Davide Marin	Creazione documento e inizio stesura

Indice

Lista delle immagini

1. Guida al deploy di GravityZone

Questa guida ha lo scopo di essere più diretta e semplice possibile, per permettere un'installazione semplice e veloce di GravityZone. La guida ufficiale e completa è invece disponibile **qui**.

1.1. Accedere a GravityZone Control Center

Questa è la parte più semplice, ma fondamentale. Collegarsi alla pagina di login di GravityZone, e inserire le credenziali relative al proprio account, impostare il 2FA o SSO e continuare.

A questo sarà necessario creare almeno un pacchetto di installazione per i nostri agent che dovremo installare sugli endpoint, per vedere come creare un pacchetto di installazione, fare riferimento al paragrafo "7.1 Creazione Installation Packages".

1.2. Installare Security Server (solo per endpoint con poche risorse)

Security server può essere installato su uno o più host, in base a quante macchine si devono gestire. L'host con security server installato centralizza la maggior parte delle attività anti-malware, e si comporta come un server per scansionare le macchine, alleggerendo il carico sulle macchine.

Per installarlo, innanzitutto scaricare il pacchetto di installazione di Security Server di default, poi, installarlo sul endpoint che si vuole utilizzare come Security Server.

Successivamente è richiesto di configurare il Security Server si può fare tramite interfaccia locale, guida ufficiale dettagliata disponibile **qui**, oppure tramite "sva-setup command", con guida ufficiale dettagliata disponibile **qui**.

1.3. Installare gli agenti

Per garantire la sicurezza degli endpoint (fisici e virtuali), è necessario installare l'agente di sicurezza su ciascun dispositivo. GravityZone offre diversi metodi per l'installazione degli agenti:

- **Installazione locale:** Si scarica il pacchetto di installazione e si installa manualmente sugli endpoint.
- **Installazione da remoto:** Modalità in cui mi concentrerò in questa guida.

1.3.1. Installazione da remoto

È importante che al primo endpoint sul quale andiamo ad installare l'agente venga assegnato il ruolo di Relay, questo per poter installare da remoto gli agenti sugli altri endpoint. Inoltre, l'endpoint che ha il ruolo di Relay deve essere sempre acceso e connesso alla rete per permettere agli altri endpoint di comunicare con il Control Center.

Una volta installato l'agente con ruolo Relay e creato un pacchetto di installazione per gli altri endpoint. sarà possibile installare gli agenti sugli altri endpoint da remoto; per farlo, andare nella pagina "Network", selezionare dalla lista tutti gli endpoint sui quali si vuole installare l'agente, a questo punto cliccare "Action" e poi "install agent".

Nella finestra che si apre, bisogna inserire le credenziali di amministratore dell'endpoint (se si ha selezionato un gruppo di endpoint sotto ad un DC, inserire le credenziali del domain

administrator), selezionare il Relay a cui fare “affidamento” ed infine il pacchetto di installazione desiderato. Questo installerà l’agente su tutti gli endpoint selezionati.

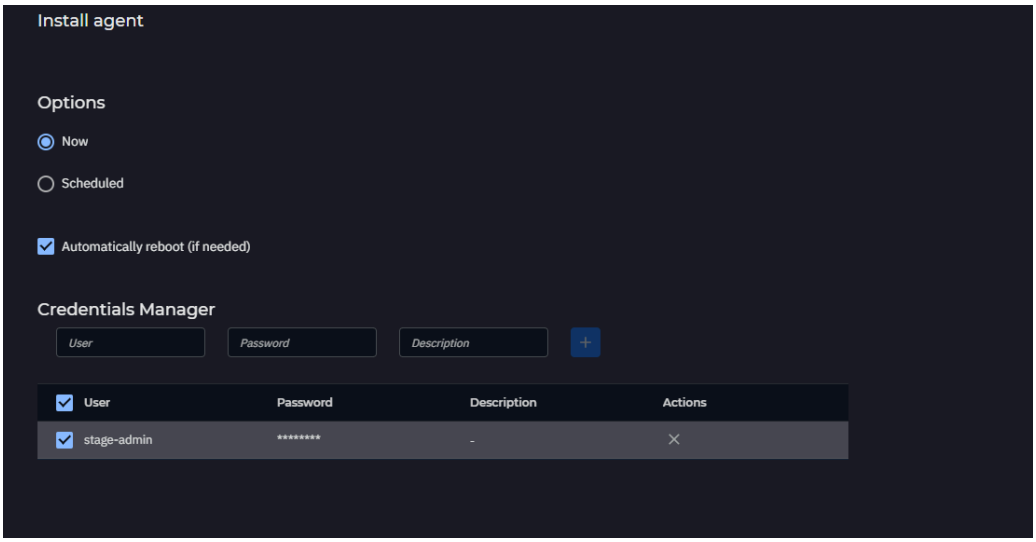

Figure 1: Installazione Agent Remoto - prima parte

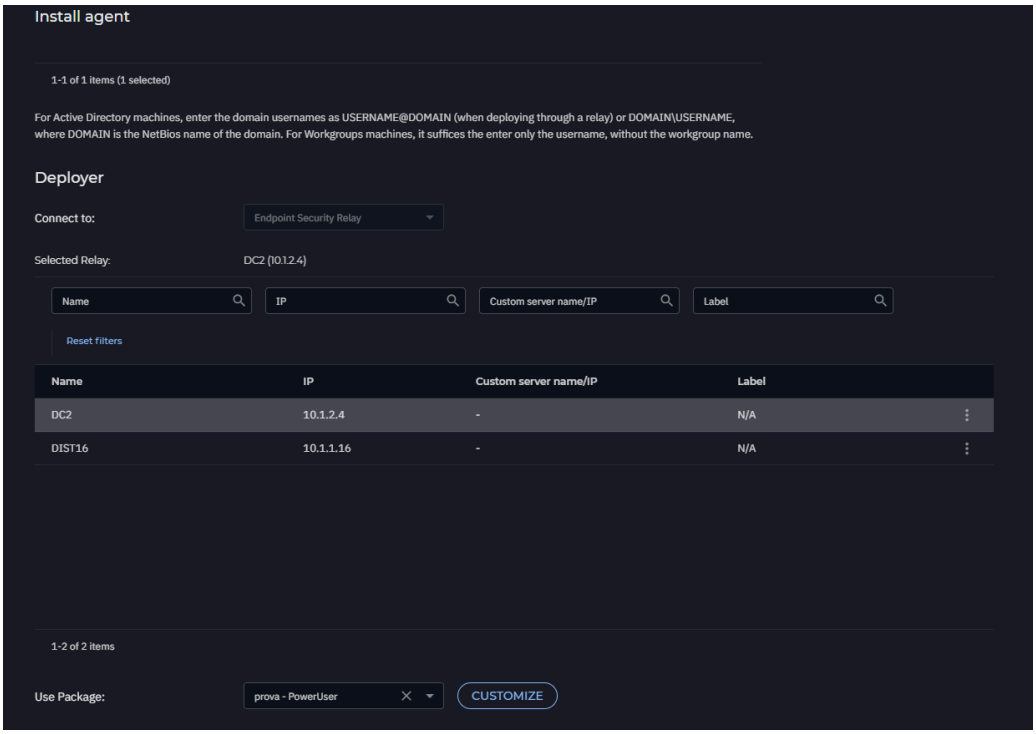

Figure 2: Installazione Agent Remoto - seconda parte

1.4. Integrazione di Active Directory

Per integrare Active Directory con GravityZone, è sufficiente accedere a GravityZone Control Center, andare nella sezione “Network” e selezionare l’endpoint che si vuole utilizzare come integratore di Active Directory. Una volta selezionato, cliccare su “Action” e poi “Set as Active Directory Integrator”.

Ora GravityZone si sincronizzerà con Active Directory ogni ora.

Per indicazioni aggiuntive e troubleshooting, è possibile consultare la guida ufficiale **qui**.

2. Guida alla creazione delle politiche di protezione

Il primo passo, è andare nella sezione “Policies” dal menu a sinistra e cliccare su “Add”.

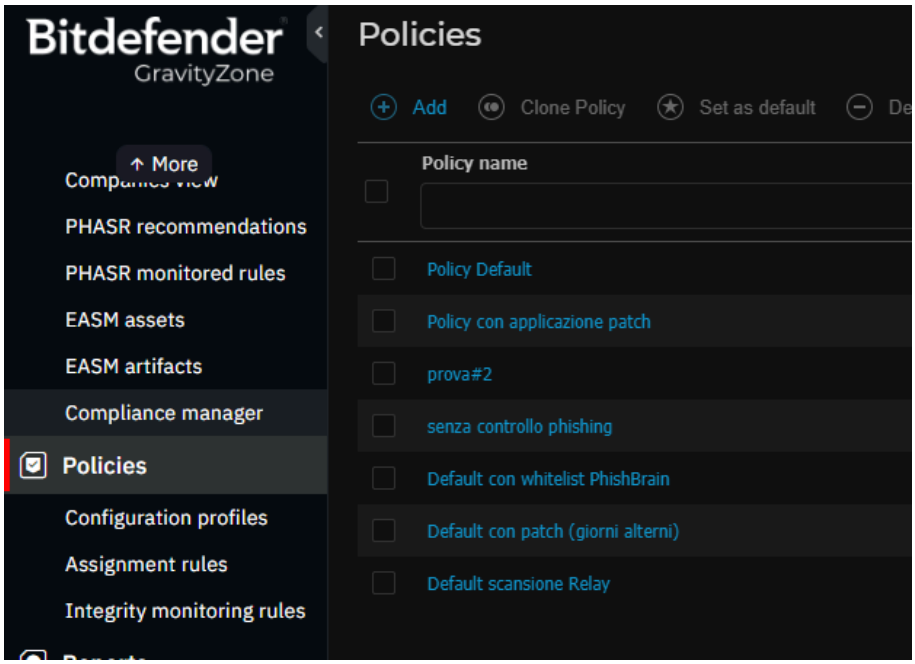

Figure 3: Aggiungi nuova politica di protezione

Dalla finestra che si apre, è possibile definire nello specifico la policy, esploriamo le varie sezioni, che si suddividono in due gruppi principali: “General” e “Protection & Monitoring”.

2.1. General

Sotto a “General” è possibile definire le impostazioni relative alla policy e agli agenti.

2.1.1. Policy

Nella sezione “Policy” è possibile definire le informazioni base della policy.

- **Details:** Qui è possibile definire il nome della politica e se essa è collaborativa o meno. È inoltre possibile inserire i contatti del supporto tecnico visualizzati dagli utenti sui loro endpoint, che di base sono quelli del supporto ufficiale di Bitdefender.
- **Inheritance Rules:** In questa pagina è possibile scegliere se “ereditare” la configurazione di un determinato modulo da un’altra policy. Attenzione, scegliendo di ereditare le regole da un’altra policy, si andrà a creare “un puntatore” alla policy da cui si ereditano le regole, e non una copia delle regole; modificando la policy da cui si ereditano le regole quindi, le modifiche verranno applicate anche a quella corrente.

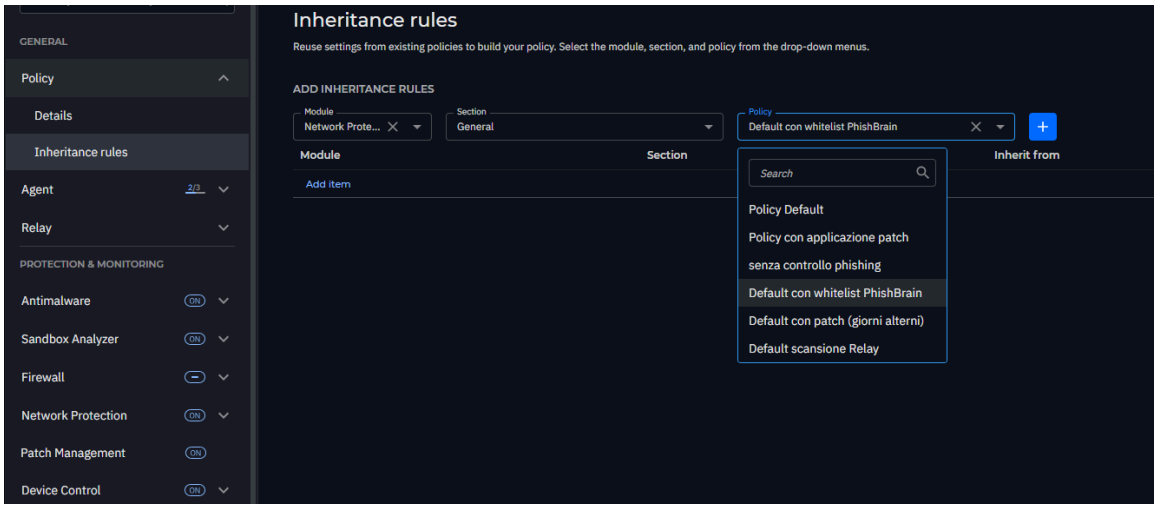

Figure 4: Aggiungi ereditarietà di un modulo

2.1.1.1. Best Practices

Per la configurazione della voce "Policy", si consiglia di non aggiungere regole di ereditarietà, a meno che non si sia sicuri che le possibili modifiche apportate in futuro al modulo della policy "madre" vadano bene anche per la policy corrente; in tutti gli altri casi, è consigliato clonare la policy madre per poter lavorare sulle due politiche indipendentemente.

2.1.2. Agent

Nella sezione "Agent" è possibile definire le impostazioni relative agli agenti che utilizzeranno questa policy.

- **Notifications:** In questa pagina si possono scegliere quali notifiche vedranno gli utenti sui loro endpoint; è possibile scegliere sia la tipologia di notifica, sia per quali eventi mostrarle.
- **Settings:** In questa pagina è possibile definire alcune impostazioni riguardanti l'installazione e i permessi dell'agente. È possibile infatti inserire impostare una password per limitare la disinstallazione dell'agente, impostare il server di proxy se presente, e rendere o meno l'agente un "Power User". Il Power User è un utente che, tramite console, può gestire le proprie impostazioni della policy.

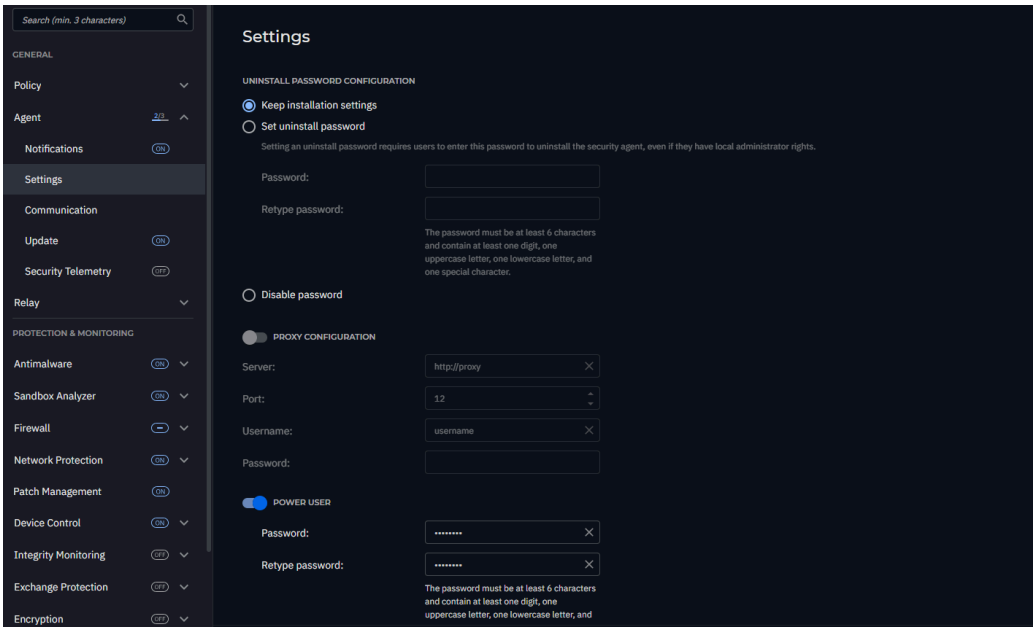

Figure 5: Impostare il power user

- **Communication:** Qui è possibile impostare con quale endpoint con ruolo "Relay" comunicare, e impostare diverse priorità in caso ci fossero più Relay. Impostare la comunicazione con il relay aiuta ad alleggerire il carico di lavoro sugli endpoint, delegando la comunicazione con il Control Center al relay.
- **Update:** In questa pagina è possibile definire le impostazioni relative agli aggiornamenti degli agenti, come ad esempio la frequenza di aggiornamento del prodotto e dei sistemi di sicurezza.
- **Security Telemetry:** In caso si disponesse di un server SIEM (soluzione di gestione delle informazioni e degli eventi di sicurezza), è possibile configurare la comunicazione con quest'ultimo in questa pagina.

2.1.2.1. Best Practices

Per quanto riguarda la sezione "Agent", si consiglia per i diversi punti:

- ***Notifications:** impostare solo di tipo "notification pop-up" (non richiedono input utente) e solo per gli eventi che interessano direttamente l'utente (es. blocco applicazione o dispositivo), lasciare invece il controllo degli incidenti malware al team di sicurezza tramite Control Center, per non allarmare inutilmente gli utenti in caso di falsi positivi. Disattivare le notifiche dei moduli che non si vogliono utilizzare.*

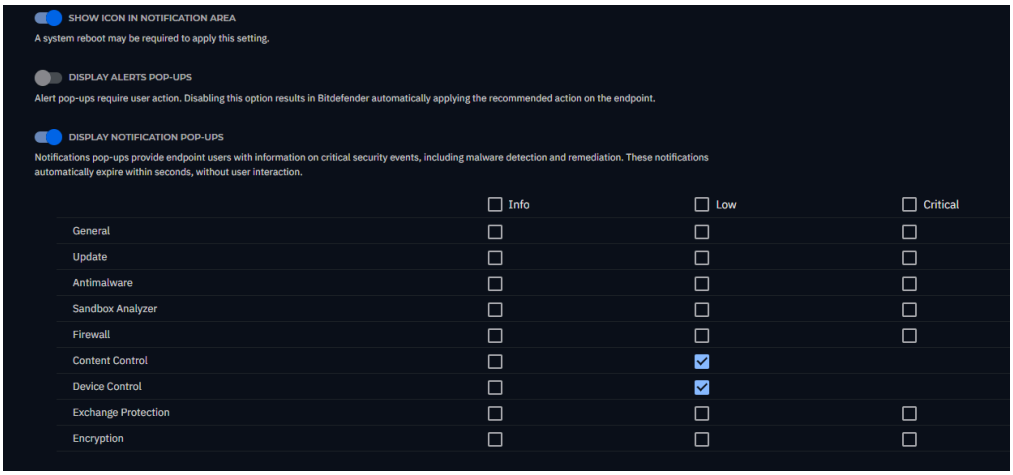

Figure 6: Esempio notifiche Agent

- ***Settings:*** *impostare la password di disinstallazione. A meno di casi particolari, non impostare l'agente come Power User.*
- ***Communication:*** *impostare tutti i Relay come endpoint di comunicazione, assegnandogli la stessa priorità, in modo da far scegliere a Bitdefender quale Relay utilizzare in base alla disponibilità.*
- ***Update:*** *lasciare le impostazioni di default.*

2.1.3. Relay

Qui è possibile vedere le impostazioni relative agli endpoint con ruolo relay, in particolare è possibile impostare i server di proxy e le location di update (che normalmente è il cloud di bitdefender).

2.1.3.1. Best Practices

Il consiglio, per quanto riguarda la sezione relay, è quello di mantenere le impostazioni di default, andando ad aggiungere i server di proxy, se disponibili, nella sezione Relay -> Communication.

2.2. Protection & Monitoring

In questa sezione viene definita la politica vera e propria, che è composta da diversi moduli:

2.2.1. Antimalware

Il modulo antimalware è molto completo, e diviso in diverse sezioni:

- **On-Access:** In questa sezione è definito il livello di aggressività della scansione che avviene al momento dell'accesso ai file.
- **On-Execute:** In questa sezione è definito il livello di aggressività della scansione che avviene al momento dell'esecuzione dei file eseguibili. Inoltre è possibile attivare o disattivare alcuni tipi di controlli, come quello per gli attacchi fileless o ransomware.
- **On-Demand:** Qui è possibile creare una regola di scansione, sono disponibili delle tipologie predefinite, come quick o full scan, oppure è possibile crearla custom, per personalizzare più a fondo la scansione (scegliere su quali cartelle effettuarla, la profondità e minutezza, ecc.). In questa schermata inoltre, premendo su "Edit" all'interno del paragrafo "Contextual Scan", si possono personalizzare le impostazioni di scansione per le cartelle locali e quelle di dispositivi esterni.

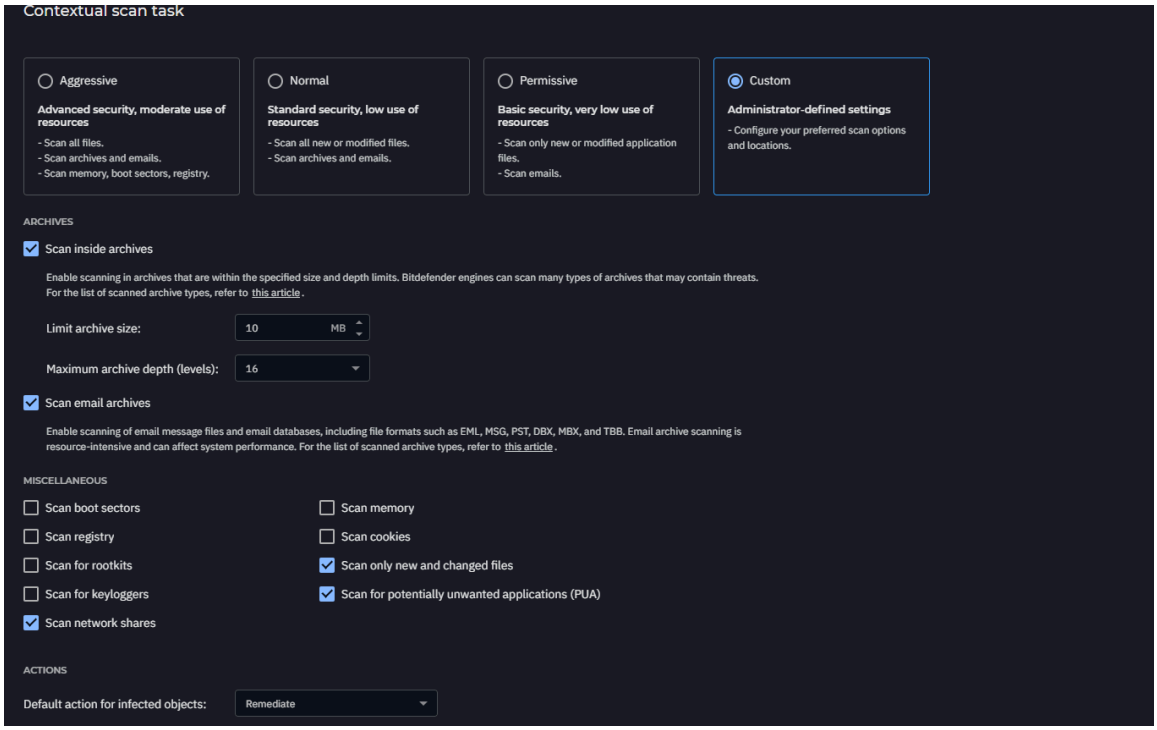

Figure 7: Impostazioni di scansione

- **Anti Tampering:** Qui è possibile attivare o disattivare i controlli anti-tampering, in particolare sui driver sensibili e sulle call-back evasion.
- **Hyper Detect:** In questa pagina è possibile attivare e configurare per quali minacce utilizzare Hyper Detect, un sistema di analisi di Bitdefender basato su machine learning.
- **Advanced Anti-exploit:** Qui si possono gestire i controlli su diversi tipi di exploit,
- **Security Servers:** Qui è possibile associare un security server alla policy, per farlo è sufficiente selezionare il Security Server desiderato dal menu a scomparsa e premere "+".
- **Settings:** Qui sono disponibili alcune opzioni aggiuntive per la policy, in particolare relativi alla quarantena dei file.
- **Exclusions:** Qui è possibile creare delle esclusioni per determinati file ,applicazioni o processi, oppure è possibile associare una lista di esclusioni precedentemente creata, per vedere come crearne una, fare riferimento al paragrafo "7.4 Creazione liste di esclusioni"

2.2.1.1. Best Practices

Per quanto riguarda il modulo antimalware, il consiglio è quello di attivare tutti i controlli disponibili (di default dovrebbero tutti essere attivi tranne la mitigazione ransomware all'interno di "On-Execute"). Per quanto riguarda lo scan On-Demand, è consigliato impostare una full scan, magari a giorni alterni, in un momento in cui le macchine sono accese ma non utilizzate (la scansione NON impedisce nessuna operazione sulla macchina, ma potrebbe appesantirne il carico di lavoro).

2.2.2. Sandbox Analyzer

Il sandbox analyzer permette di analizzare i file sospetti in un ambiente sicuro, attivando la funzione, verranno inviati automaticamente al sandbox i file individuati. Per vedere il funzionamento del sandbox, fare riferimento al paragrafo "7.6 Utilizzo del Sandbox Analyzer"

2.2.2.1. Best Practices

Si consiglia di attivare la funzione, mantenendo però la "analysis mode" su "Monitoring" e la default action "report only", in questo modo non verranno mai bloccati file senza motivazioni certe.

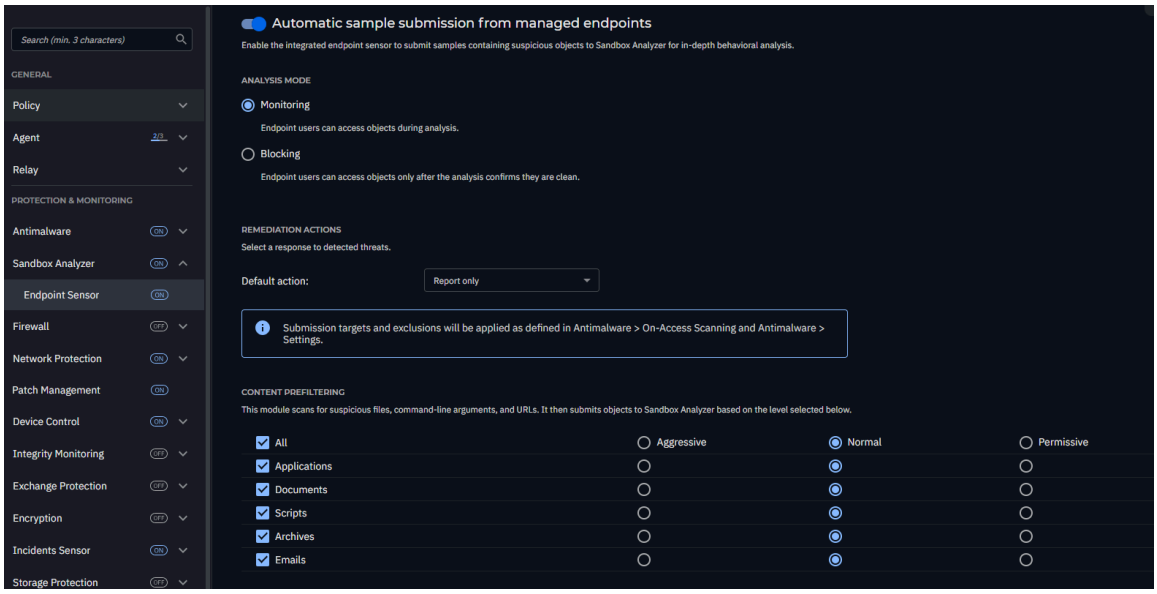

Figure 8: Configurazione Sandbox nella policy

2.2.3. Firewall

Il firewall di bitdefender permette di controllare le connessioni in entrata e in uscita direttamente sul endpoint.

- **General:** Qui è possibile attivare il firewall e decidere se controllare anche le connessioni wi-fi e lo scanning delle porte inserendo anche eventuali esclusioni.
- **Settings:** Qui è possibile creare diverse categorie di rete (ufficio, casa, fidata, ecc.) per poi potergli affidare diverse regole di controllo.
- **Rules:** Qui è possibile creare le regole di controllo e assegnarle alle varie categorie di rete.

2.2.3.1. Best Practices

Per quanto riguarda il firewall, in caso il cliente disponesse già di un firewall esterno è possibile anche disattivare il modulo, ricordandosi di deselezionare la spunta "Firewall" all'interno della sezione Agent -> Notifications. In caso si volesse mantenere il firewall invece, lasciare le impostazioni di default ricordandosi di aggiungere le porte da escludere in Firewall -> General. Creare le categorie desiderate in Firewall -> Settings e poi tutte le regole necessarie in Firewall -> Rules

2.2.4. Network Protection

Il modulo Network Protection permetta di applicare filtri e controlli su web e applicazioni.

- **General:** Qui si imposta se controllare o meno anche il traffico criptato e di quale tipo, e si aggiungo le eventuali esclusioni ai controlli (sia URL o IP sia applicazioni), se le esclusioni sono molte e saranno applicate a più policy, è possibile creare delle "custom exclusion rules", per vedere come fare, fare riferimento al paragrafo "7.8 Custom Exclusion Rules".

- **Content Control:** Nella schermata content control è possibile attivare il controllo web, selezionando una regola precedentemente creata, per farlo seguire la guida al paragrafo "7.3 Creazione Web Access Control Scheduler". È anche possibile creare una blacklist di applicazioni per impedirne l'esecuzione. Infine, è possibile inserire una lista di dati sensibili, questa lista bloccherà l'invio di questi dati scansionando tutte le tipologie di traffico spuntate nella sezione Network Protection -> General, in caso di blocco l'utente visualizzerà un alert.
- **Web Protection:** Qui è possibile attivare il controllo phishing, il controllo web in real time e la scansione email.
- **Network Attacks:** Qui è possibile attivare e impostare la difesa dagli attacchi web. È possibile scegliere per ogni tipologia di attacco se bloccarne l'accesso o creare solamente un alert nel Control Center.

2.2.4.1. Best Practices

- ***General:*** *Attivare la scansione del traffico criptato e anche il controllo https. Aggiungere alle esclusioni siti e applicazioni utilizzati frequentemente e/o sensibili (es. banca, gestionali, ecc.).*
- ***Content Control:*** *se presente, assegnare al web access control la schedule creata precedentemente come spiegato nel paragrafo "7.3 Creazione Web Access Control Scheduler". In caso si volessero aggiungere dei dati sensibili al Data Protection, si consiglia di non aggiungere, ad esempio, una password per intero, ma piuttosto una sua parte univoca (es. con password "Psd!23@" inserire "!23@").*
- ***Web Protection:*** *Mantenere le impostazioni di default, ovvero tutto attivo tranne il controllo mail (senza exchange protection configurato non ha alcun effetto).*
- ***Network Attacks:*** *Attivare RDP traffic e settare tutti i controlli su "block".*

2.2.5. Patch Management

Qui è possibile associare alla policy una maintenance window creata precedentemente, per crearne una fare riferimento al paragrafo "7.2 Creazione Maintenance Windows".

Le maintenance windows definiscono le politica di scansione e applicazione delle patch sugli endpoint associati.

2.2.6. Device Control

Il modulo Device Control permette di bloccare l'accesso a determinate categorie di dispositivi (archiviazione esterna, bluetooth, ecc.), ma anche per tipologia di periferica (chiavette USB, PCI, ecc.).

- **Rules:** Nella schermata rules è possibile bloccare determinati tipi di dispositivi divisi per categorie. È possibile anche bloccare una sola tipologia di periferica senza bloccare l'intera categoria. Per farlo selezionare la categoria, premere su custom, e settare su "block" solo quella tipologia (ad esempio, per bloccare le chiavette USB, selezionare "External Storage", selezionare l'opzione "Custom" e settare solo "USB" su "Blocked").

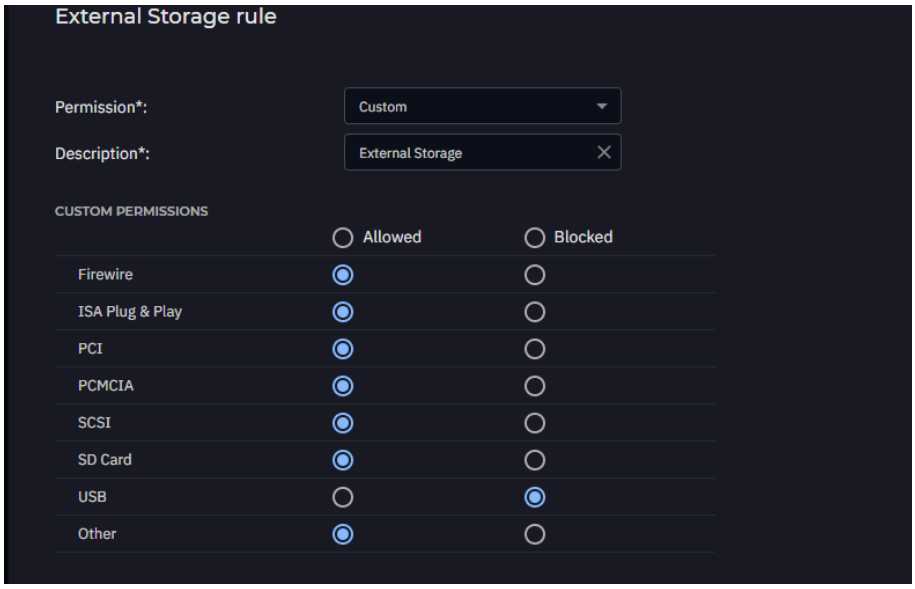

Figure 9: Device Control

- **Exclusions:** Qui è possibile aggiungere determinati dispositivi "fidati" che potranno essere utilizzati nonostante le regole di blocco, si possono inserire da dispositivi già conosciuti, oppure manualmente tramite ID.

2.2.6.1. Best Practices

Collegare prima i dispositivi fidati e dopo attivare il blocco, in questo modo sarà possibile aggiungerli nelle esclusioni direttamente da "from discovered devices".

2.2.7. Incident Sensor

Questo modulo è fondamentale per poter utilizzare la funzionalità di rilevamento incidenti, e relativa pagina "Incidents" nel menu a sinistra.

2.2.8. Risk Management

Questa pagina permette di configurare la regola di scansione dei rischi, queste scansioni individuano vulnerabilità date da impostazioni delle applicazioni o da registri di sistema inutilizzati, inoltre individuano anche il rischio associato ad ogni utente. Sempre in questa schermata è possibile abilitare il PHASR, sistema di machine learning che, dopo un periodo di training (circa 30 giorni), fornisce consigli su che modifiche applicare ai vari utenti per migliorarne la sicurezza.

2.2.8.1. Best Practices

Impostare la scansione anche ogni giorno, meglio in orari dove il computer non è utilizzato, ma è una scansione più leggera rispetto ad una full scan. Consigliato è anche attivare il PHASR, impostando tutto su "Direct Control", in questo modo non verranno applicate le misure individuate automaticamente, ma saranno solo consigliate e attenderanno approvazione.

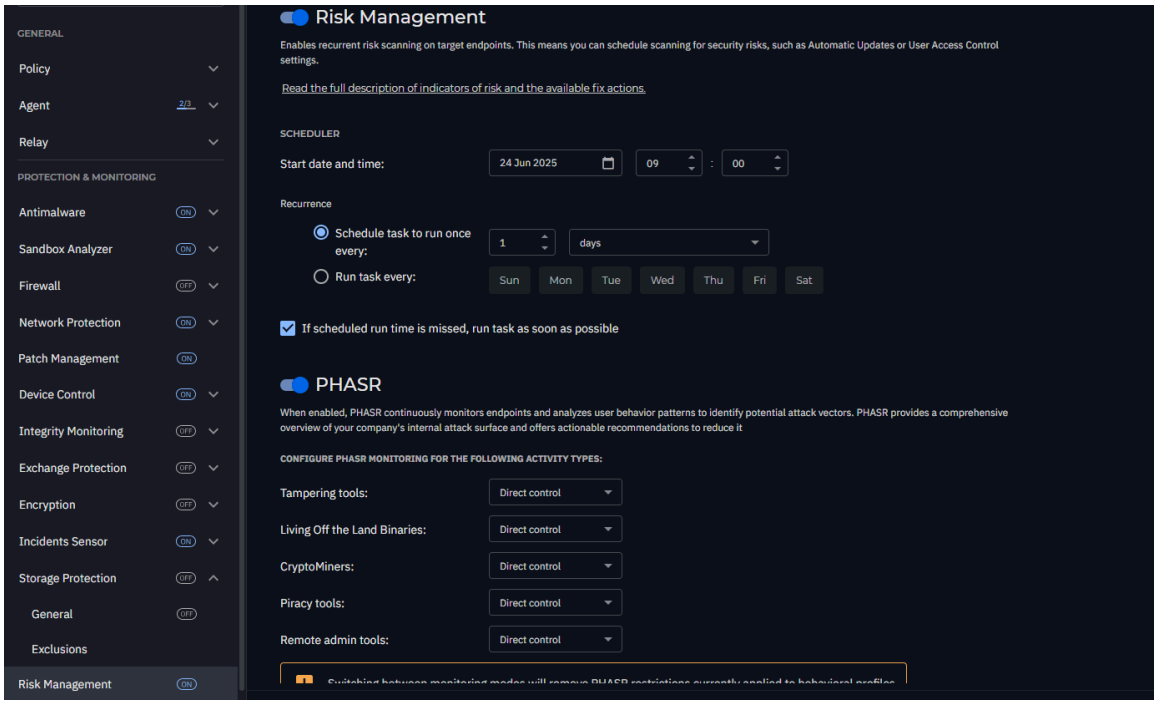

Figure 10: Configurazione Risk Management

2.2.9. Blocklist

Nella pagina blocklist è possibile configurare quali controlli delle liste, create nella sezione "Blocklist" del menu a sinistra, saranno efficaci su questa policy. Per vedere come creare una blocklist, fare riferimento al paragrafo "7.5 Creazione delle Blocklist".

Disattivando "Application path" ad esempio, se fossero presenti delle applicazioni inserite nella blocklist, esse non sarebbero bloccate per gli utenti con questa policy.

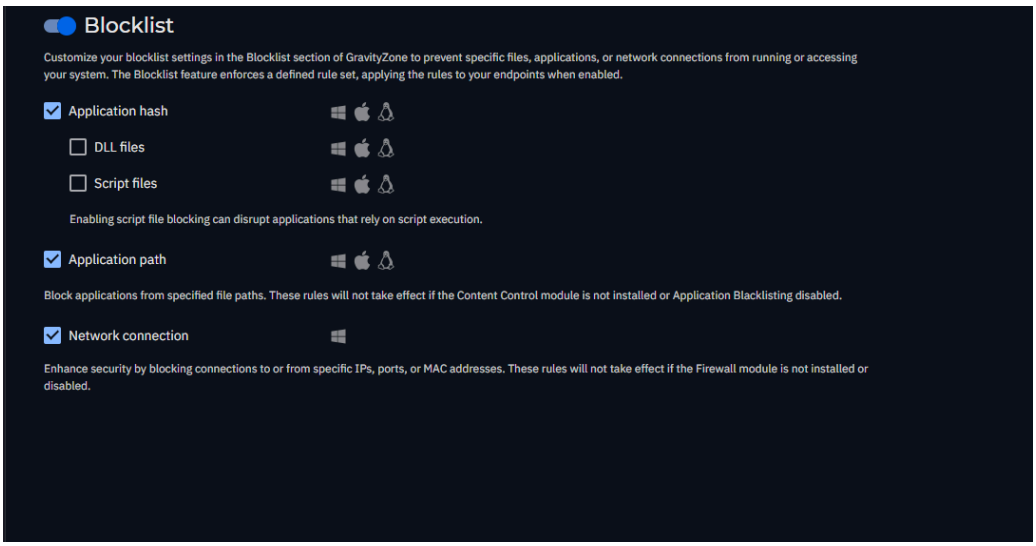

Figure 11: Configurazione Blocklist

2.2.9.1. Best Practices

Spuntare tutte le tipologie di controllo, tranne DDL files e Script files per non causare problemi durante l'esecuzione delle applicazioni. Ricordarsi che alcuni di questi controlli dipendono

anche dall'attivazione del modulo della rispettiva categoria (es. Network connection non funzionerà se il firewall è disattivato).

2.2.10. Live Search

Attivando la live search si rende possibile effettuare delle query per ottenere informazioni sugli endpoint. Le informazioni possono essere utili per la diagnostica in caso di incidenti nella rete. Per effettuare le ricerche in tempo reale è necessario creare le query nella pagina "Incidents -> Search" del menu a sinistra.

2.2.10.1. Best Practices

Si consiglia di attivarla, in quanto non comporta nessun carico extra finché non vengono eseguite delle query dalla schermata apposita.

3. Guida alla gestione dei tag

3.1. Creazione del tag

I tag sono sono uno strumento utile che permette di raggruppare gli endpoint per diversi criteri, per poi assegnare le policy di protezione direttamente ai gruppi risparmiando tempo e semplificando l'operazione.

Per creare un tag, andare in "Network -> Tags management" dal menu a sinistra, a questo punto premere su "Add tag". Nella schermata che si apre è possibile creare un tag in modalità custom, ovvero sarà necessario poi scegliere manualmente a quali endpoint assegnarlo, oppure in modalità automatica, ovvero il tag sarà assegnato automaticamente in base ai filtri inseriti di seguito.

Selezionando "Automatic", sarà possibile inserire i filtri per nome (anche con wildcard), IP, sistema operativo e tipologia di endpoint (workstation/server/ecc.). Inserendo più filtri, il tag si applicherà agli endpoint che li rispettano tutti.

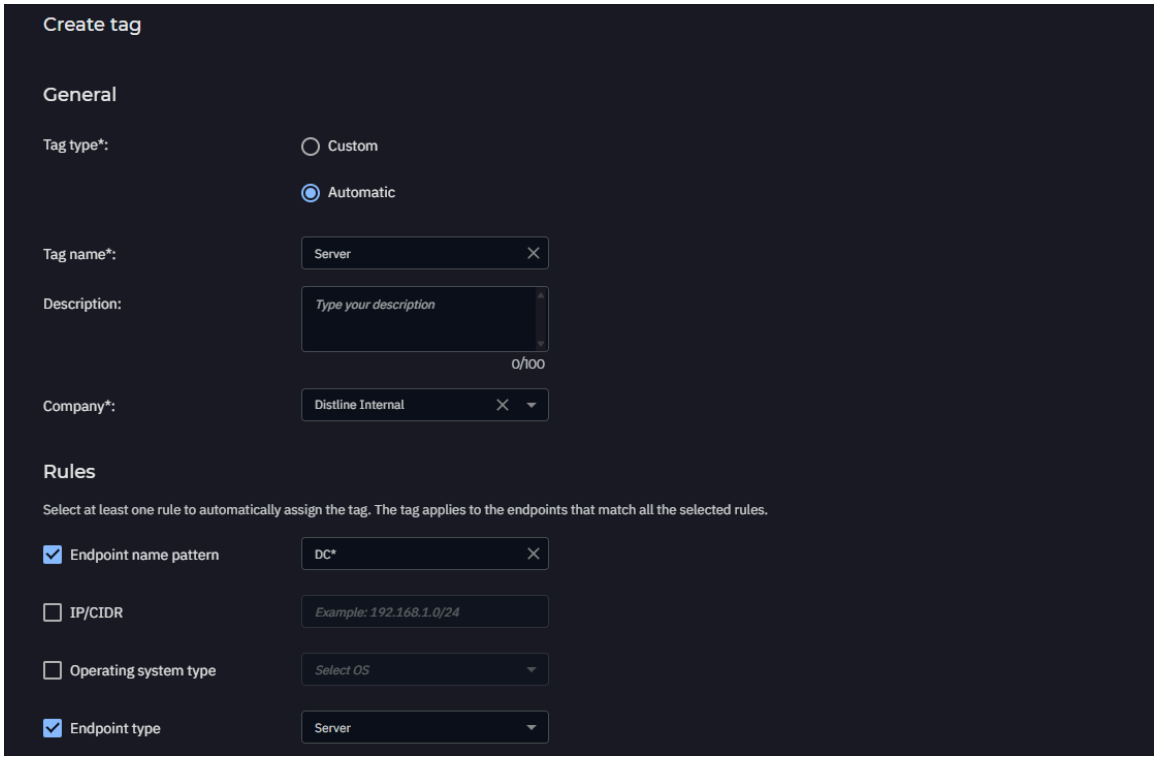

Figure 12: Creazione Tag

Se si è creato un tag "Custom" invece, sarà necessario andare nella sezione "Network" e selezionare dalla lista degli endpoint tutti quelli a cui vogliamo assegnare il tag, una volta selezionati premere "Action -> Assign tags" e selezionare il tag desiderato.

3.2. Associazione di tag e policy

Per associare il tag alla policy desiderata sarà sufficiente andare nella sezione "Policy -> Assignment Rules", in questa schermata premere su "Add -> Endpoint tag rule". Nella finestra che si è aperta, compilare i campi in base alla policy e al tag che si vuole associare

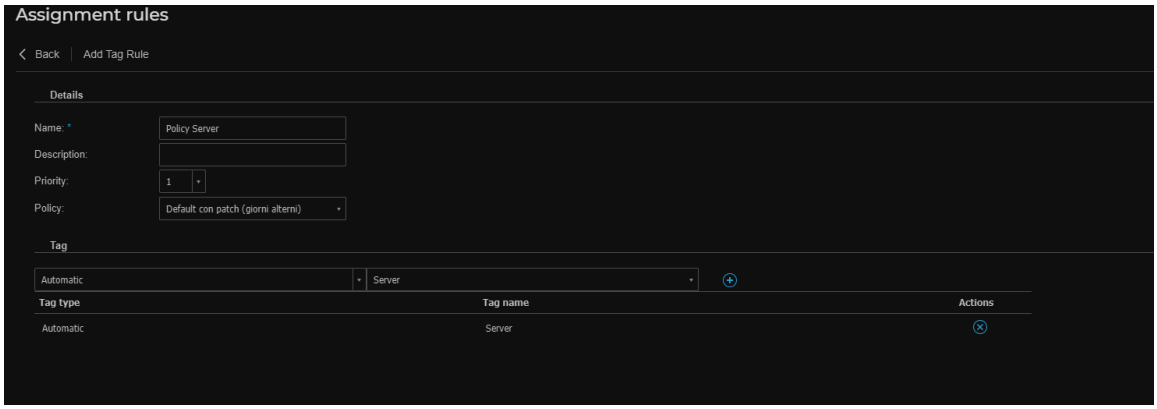

Figure 13: Creazione Assignment Rule

4. Guida al patch management

La funzione di patch management di GravityZone trova bug, errori di configurazione e obsolescenze che possono essere sfruttati per degli attacchi, e ne ricerca le patch, permettendo poi di installarle in automatico.

GravityZone mette a disposizione uno strumento per eseguire scansioni delle patch disponibili per le proprie macchine, è possibile avviarle manualmente (on-demand) selezionando la macchina desiderata nella sezione “Network” e premendo su “Action -> Patch Scan”, oppure è possibile farle eseguire automaticamente creando prima una “Maintenance Window” e poi assegnandola alla policy, per vedere come crearla, far riferimento al paragrafo “7.2 Creazione Maintenance Window”.

Una volta che gli endpoint eseguiranno le scansioni patch, sarà possibile visualizzare la lista di tutte quelle trovate nella sezione “Network -> Patch Inventory” del menu a sinistra. Direttamente in questa schermata, sarà possibile spuntare le patch desiderate e poi premere su “Install” per installarle su tutti gli endpoint che le richiedono. Se nella maintenance window si è spuntata l’opzione “Patch Install”, questa operazione sarà necessaria solo per alcune patch che richiedono approvazione manuale.

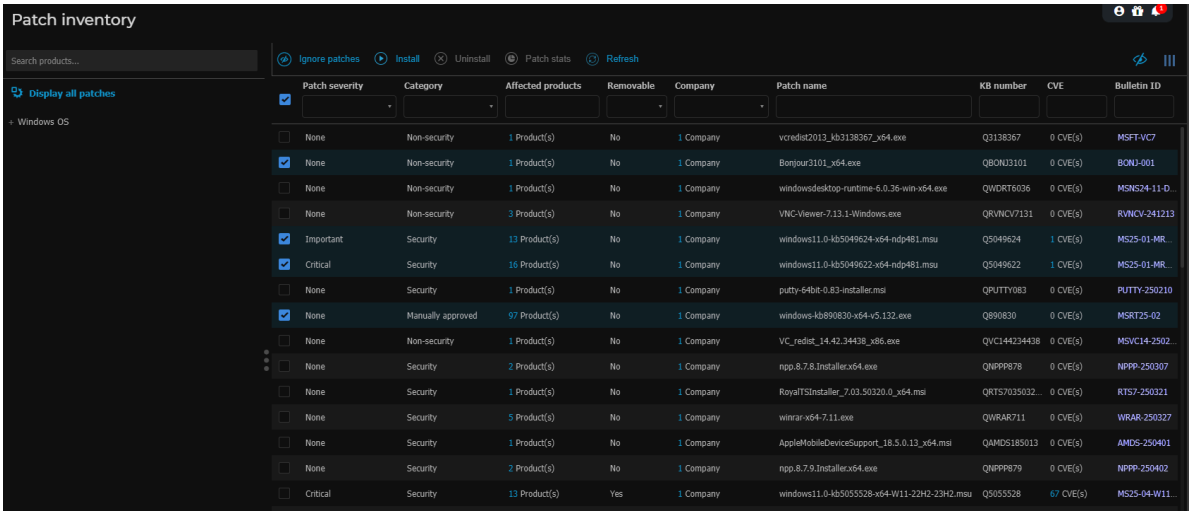

Figure 14: Patch Inventory

Per avere una panoramica dello stato delle patch su ogni endpoint, è possibile creare un report apposito chiamato “Network Patch Status”, per vedere come creare un report, fare riferimento al paragrafo “5 Gestione dei Report”.

5. Gestione dei Report

GravityZone permette di controllare lo stato degli endpoint, della rete e anche del servizio attraverso un grande numero di report.

5.1. Creazione di Report

È possibile creare un report andando nella sezione “Reports” del menu a sinistra, nella pagina che si apre premere “Add”. Nella schermata che si apre, selezionare il tipo di report desiderato dalla lista proposta, per alcuni tipi di report saranno disponibili ulteriori filtri una volta selezionati.

A questo punto è possibile scegliere se generare un report rapido, che sarà visualizzato direttamente in questa pagina, oppure aggiungere una schedule e inviarlo per mail agli indirizzi desiderati con ricorrenza e orari a piacere.

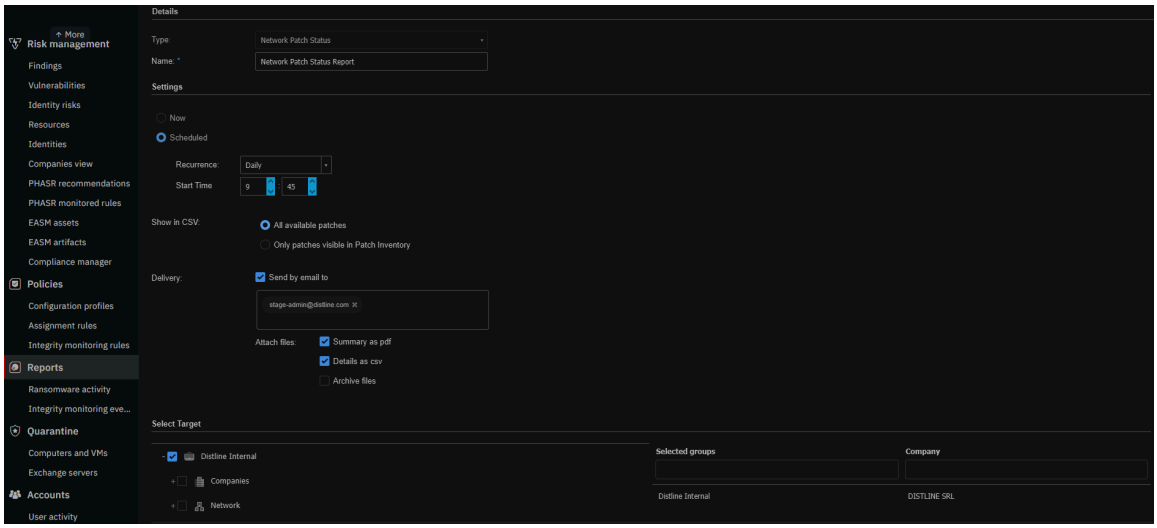

Figure 15: Report Schedule

5.2. Creazione report per singoli endpoint o gruppi

Se si volesse creare un report per uno specifico endpoint o un gruppo, è possibile farlo dalla sezione “Network” del menu a sinistra. Una volta che si visualizza la lista degli endpoint, è possibile selezionare gli endpoint desiderati e poi premere su “Reports”.

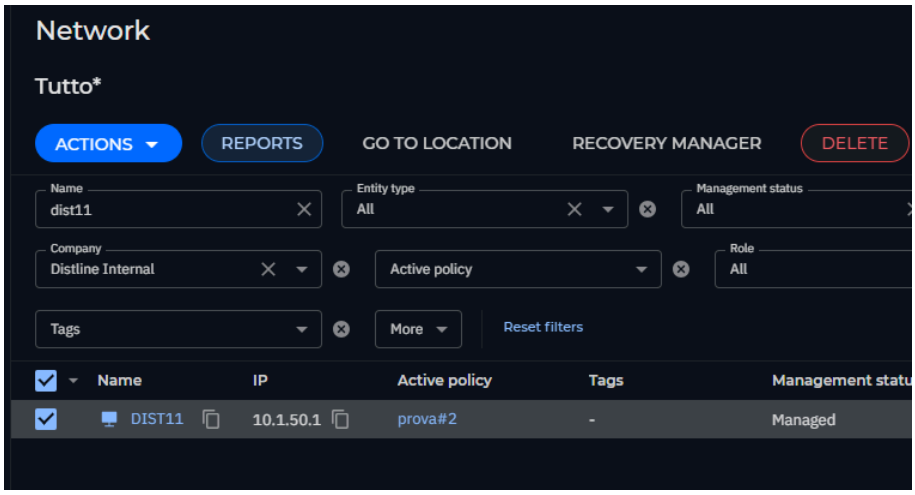

Figure 16: Report Singolo Endpoint

Attenzione, in questo caso i report saranno solo di tipo rapido, non è possibile infatti creare schedule di report per singoli endpoint o gruppi.

5.3. Best Practices

Nella creazione di report con schedule, il file PDF solitamente ha una panoramica molto riassuntiva dei dati del report, se si volessero numeri e dati precisi (spesso suddivisi anche per endpoint), è consigliato allegare anche il file CSV.

6. Risk Management

GravityZone mette a disposizione anche uno strumento per visualizzare tutte le vulnerabilità trovate sui vari endpoint, che non rispettano le varie tipologie di compliance. È possibile visualizzare i rischi dovuti a impostazioni di applicazioni o registri di sistema, gestione degli utenti, o alle versioni vulnerabili di applicazioni.

6.1. Findings

All'interno della sezione "Risk Management -> Findings" del menu a sinistra, è possibile visualizzare la lista di tutte le vulnerabilità, trovate nei vari endpoint, relative a impostazioni di applicazioni o a registri di sistema, per ogni finding è inoltre disponibile un dettaglio che spiega cosa fare per risolverlo. Sono disponibili anche vari filtri per ricercare le vulnerabilità desiderate.

Da questa schermata, inoltre, è possibile risolvere le vulnerabilità trovate (se esse sono risolvibili automaticamente), per farlo selezionare le vulnerabilità desiderate e premere "Fix Issue".

6.1.1. Best Practices

In questa schermata, è possibile visualizzare ad esempio quali vulnerabilità non fanno rispettare una determinata compliance (es. ISO), per tutti o anche un determinato endpoint.

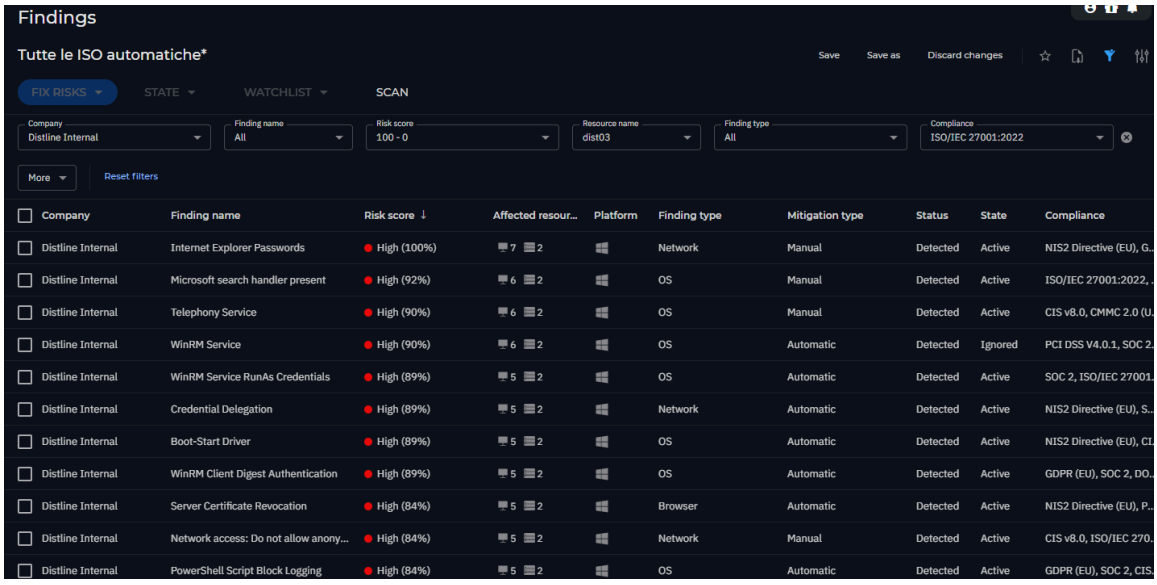

Figure 17: ISO non rispettate per singolo endpoint

6.2. Identity Risk

Similarmente a "Findings", l'identity risk evidenzia quali impostazioni degli utenti risultano in vulnerabilità e le compliance ad esse associate.

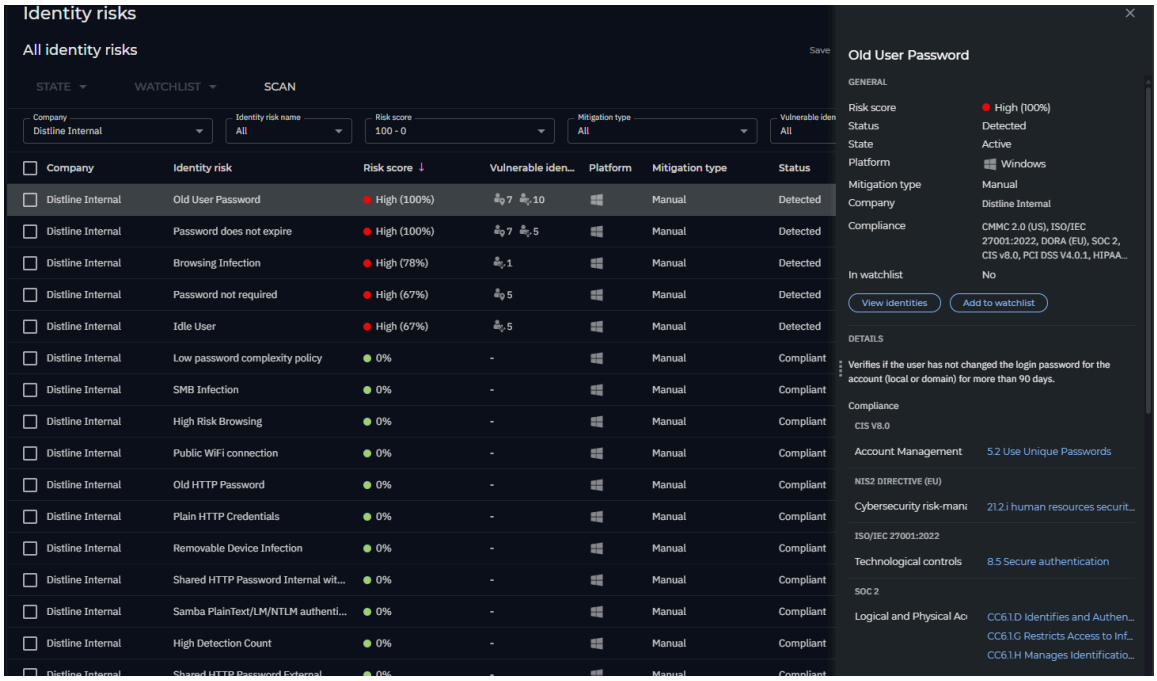

Figure 18: Identity Risk

6.3. Resources

Questa schermata elenca ogni endpoint presente nella rete associandone un livello di rischio basato sul numero di findings trovati e sul livello di rischio degli utenti che lo utilizzano.

Premendo su un endpoint, è visualizzabile la lista delle vulnerabilità trovate e quali compliance esse non rispettano.

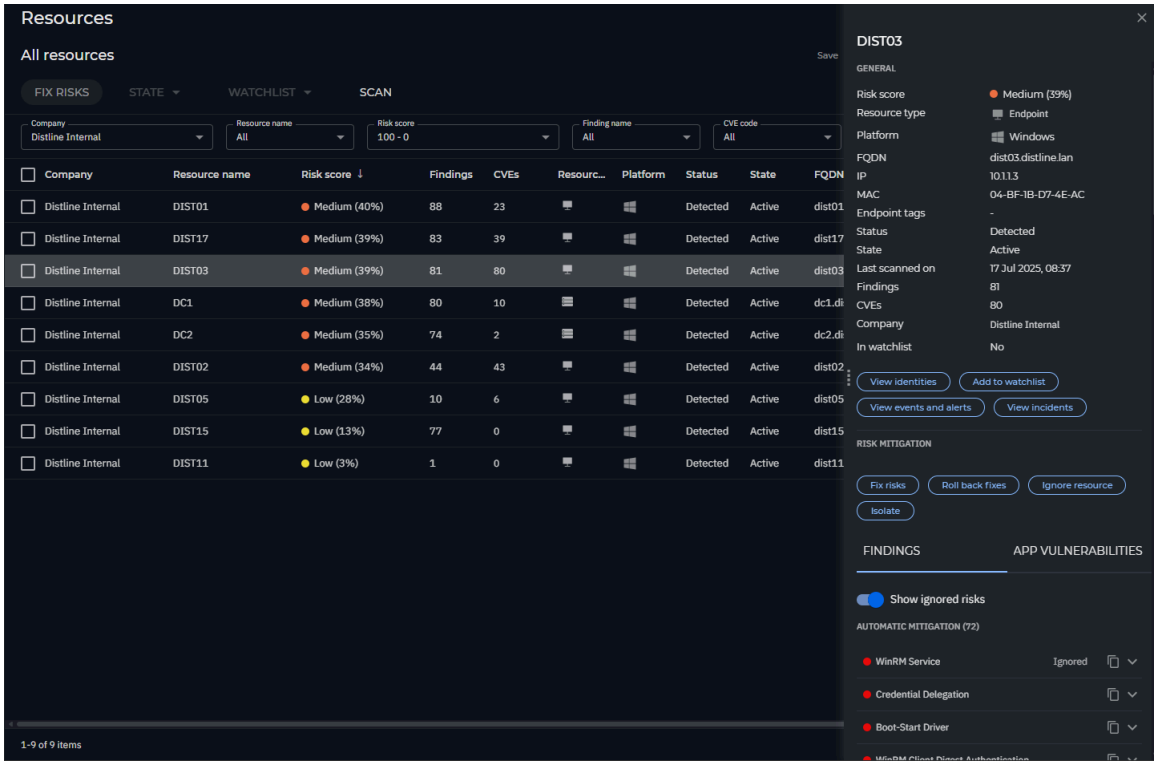

Figure 19: Resources Risk

6.4. Identities

Questa schermata elenca tutti gli utenti presenti nella rete associandone un livello di rischio basato su quanti e quali "Identity Risk" presentano.

Premendo su un utente, è visualizzabile la lista delle vulnerabilità trovate e quali compliance esse non rispettano.

6.5. Vulnerabilities

Questa schermata mostra tutte le vulnerabilità di applicazioni o sistemi operativi, per le quali però GravityZone non offre rimedio automatico. Le vulnerabilità trovate qui possono essere quindi di due tipi: patch ancora non disponibile, oppure versione dell'applicazione troppo obsoleta e va quindi aggiornata manualmente.

6.6. Compliance Manager

Infine, è possibile creare dei report per certificare il livello di compliance direttamente con Bitdefender, purtroppo per le compliance "avanzate" (come ISO ecc.) è necessaria una licenza specifica per ognuna.

6.6.1. Best Practices

Per sapere se si è compliant, basterà filtrare per le varie compliance nelle sezioni "6.1 Findings" e "6.2 Identity Risk", il report è utile soltanto per certificare lo stato di compliance.

7. Altre funzionalità

7.1. Creazione Installation Packages

I pacchetti di installazione definiscono quali moduli ed eventuali privilegi saranno attribuiti agli endpoint.

Per creare un pacchetto, andare nella sezione “Network -> Installation Packages” del menu a sinistra, nella finestra che si apre, premere su “Create”. A questo punto, nella schermata aperta, sarà possibile inserire il nome del pacchetto e selezionare tutti i moduli desiderati da essere installati. È inoltre possibile settare altre impostazioni, come richiedere una password per la disinstallazione dell’agent, se installare il pacchetto in un percorso specifico, se utilizzare un server di proxy per comunicare con il Control Center.

7.1.1. Best Practices

Per la creazione dei pacchetti, si consiglia di selezionare tutti i moduli disponibili, tranne “Power User”, in modo da rendere più agevole la gestione degli endpoint e la creazione delle policy, senza dare inutilmente privilegi agli utenti.

È consigliato impostare una password per la disinstallazione dell’agent e di spuntare “remove competitors”.

7.2. Creazione Maintenance Windows

La maintenance window definisce la politica di scansione e applicazione delle patch, una volta creata è possibile associarla alle policy desiderate direttamente nella sezione “Patch Management” all’interno della policy.

Per creare una maintenance window andare nella sezione “Policies -> Configuration Profiles” del menu a sinistra, nella finestra che si apre selezionare “Maintenance Windows”. Nella schermata che si apre premere “Add Window”, a questo punto sarà possibile decidere se solo scansionare gli endpoint, o se anche applicare le patch trovate. Per entrambe le operazioni sono disponibili le impostazioni di ricorrenza e orario di esecuzione.

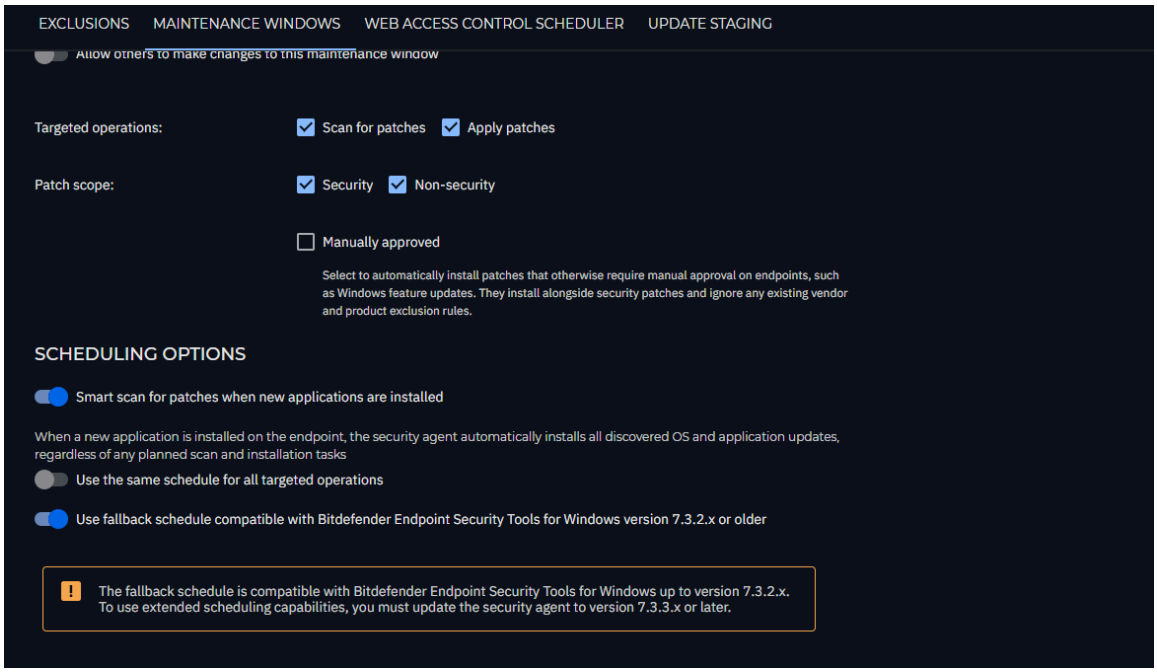

Figure 20: Maintenance Window

Se si è impostato un endpoint come server di cache per le patch qui è possibile assegnarlo alla window, in questo modo le patch saranno scaricate sul endpoint dal server di cache e non dal sito del vendor.

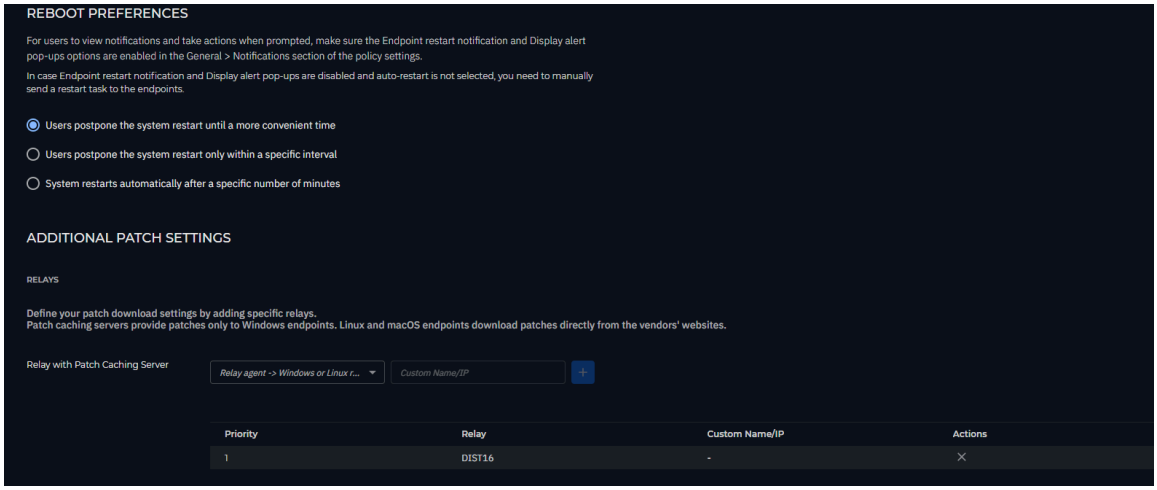

Figure 21: Patch Caching Server

7.2.1. Best Practices

Si consiglia di attivare sia la scansione sia l'applicazione delle patch, e di spuntare sia "Security" che "Non-security". Attivare anche la fallback schedule, che permette di ripristinare i prodotti alla versione precedente in caso di problemi in seguito all'applicazione patch.

Per quanto riguarda la ricorrenza, è consigliato effettuare la scansione abbastanza spesso, ad esempio una volta ogni 2 giorni e in orari in cui le macchine sono accese (in ogni caso lasciare spuntata l'opzione "if missed run ASAP").

7.3. Creazione Web Access Control Scheduler

È possibile creare un Web Access Control Scheduler dalla sezione “Policies -> Configuration Profiles” del menu a sinistra, e poi selezionando “Web Access Control Scheduler” dalla finestra che si apre.

Nella schermata che si apre, premendo “Add Schedule”, è possibile creare una o più regole di controllo. Il sistema propone categorie di siti selezionabili per il controllo (come social network, gioco d’azzardo, shopping ecc.). Per ogni regola è possibile selezionare gli intervalli di tempo per cui essa sarà in vigore e anche se bloccare completamente le pagine oppure mostrare solo un warning all’utente.

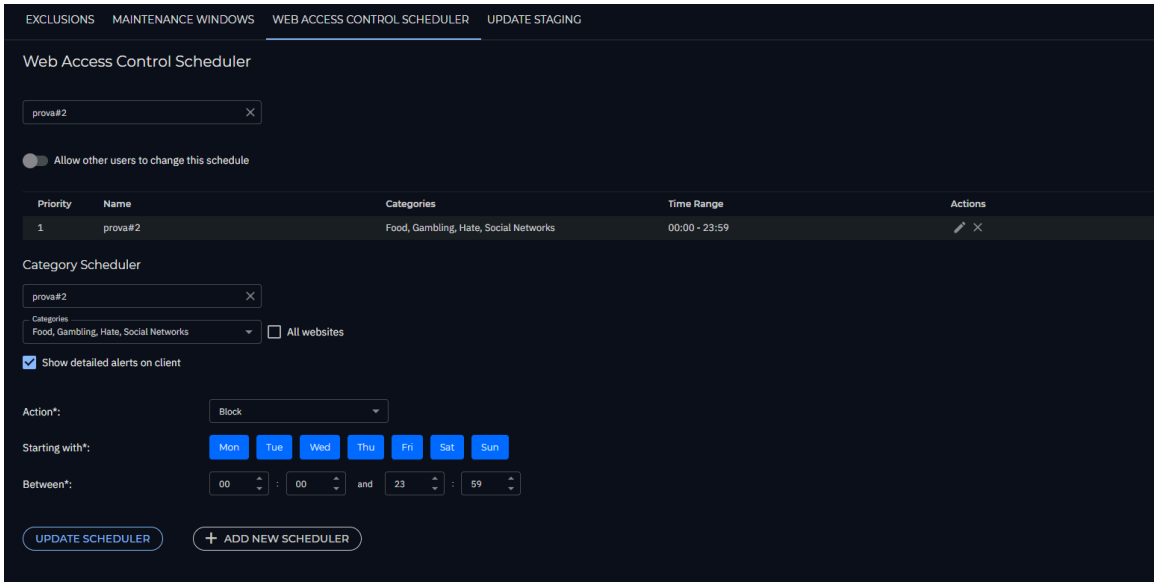

Figure 22: Creazione Web Access Control Scheduler

7.3.1. Best Practices

Perché la schedule funzioni a dovere, è necessario aver attivato la scansione HTTPS in Network Protection -> General, altrimenti le pagine con quel protocollo non saranno controllate.

Attenzione, i tentati accessi ai siti saranno mostrati nella pagina “Threats Explorer”, solo se la tipologia di action è settata su “Block”. Per vedere il funzionamento della pagina, fare riferimento al paragrafo “7.7 Threats Explorer”.“

7.4. Creazione liste di esclusioni

Tramite le liste di esclusioni, è possibile creare dei gruppi di esclusioni, in modo da poterle aggiungere a più policy in maniera rapida e semplice. Innanzitutto, andare alla sezione “Policy -> Configuration Profiles” del menu a sinistra, nella schermata che si apre selezionare “Exclusions”. Se non si ha già una lista, premere su “New List”, a questo punto inserire un nome e tutte le esclusioni che vogliamo.

Altrimenti, è anche possibile creare direttamente un’esclusione tramite pulsante “Add Exclusion”, e poi assegnarla a tutte le liste che vogliamo selezionandola dall’elenco e premendo su “Assign to Lists”.

7.5. Creazione delle Blocklist

Le blocklist permettono di avere delle liste di applicazioni o processi bloccati "prestabilite" da poter essere incluse in tutte le policy che vogliamo, senza doverle ricreare in ogni policy.

Per creare una regola, andare nella sezione "Incidents -> Blocklist" nel menu a sinistra e, nella finestra che si apre, premere "Add rule". Una volta premuto "Add Rule" ci verrà richiesto di scegliere quale tipo di blocco vogliamo creare, e poi i dettagli riguardanti l'elemento da bloccare (Percorso app, IP, ecc.).

Una volta creati i blocchi, essi saranno automaticamente aggiunti a tutte le policy che hanno attivi i corrispondenti moduli.

7.6. Utilizzo del Sandbox Analyzer

Il servizio di Sandbox utilizza degli ambenti virtuali hostati da Bitdefender per analizzare a fondo i file sospetti.

Una volta inserito nel sandbox, il file viene "detonato" all'interno di un ambiente simile in tutto e per tutto a quelli standard, evitando quindi misure di controllo invasive che possano allertare il file sospetto. L'ambiente rimane in ascolto, controllando e registrando nello specifico:

- Ogni file che è stato modificato, eliminato, creato o cambiato
- Ogni chiave del Registro di sistema modificata, creata o eliminata
- Ogni processo creato, terminato o iniettato
- Ogni istruzione API eseguita
- Ogni connessione di rete

I file sospetti vengono inviati automaticamente al sandbox se è attiva l'opzione nella policy, come spiegato nel paragrafo "2.2.2 Sandbox Analyzer".

È anche possibile inviare manualmente dei file al sandbox, direttamente dalla sezione "Sandbox Analyzer -> Manual submission" del menu a sinistra. Una volta aperta la schermata, sarà possibile selezionare il file/archivio da mandare al sandbox direttamente dalle cartelle del dispositivo, inoltre è possibile inserire la password, se necessaria, per aprire/eseguire i file inviati.

Dopo qualche minuto, il risultato del controllo sarà disponibile nella sezione "Sandbox Analyzer" del menu a sinistra. In questa schermata saranno mostrati tutti i file inviati al sandbox e relativo stato di sicurezza.

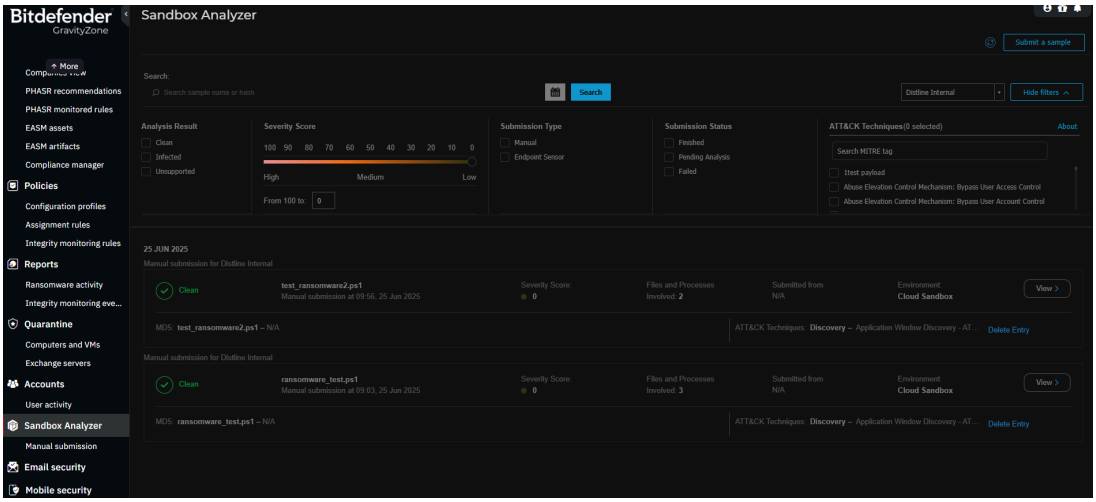

Figure 23: Risultati Sandbox Analyzer

7.7. Threats Explorer

Il threats explorer, disponibile nella sezione “Threats Explorer” del menu a sinistra, raccoglie ed elenca tutti i possibili pericoli individuati dalle diverse tecnologie di GravityZone.

Qui sono anche elencati i pericoli bloccati seguendo le impostazioni delle policy, come quelli di controllo dispositivi (es. tentato utilizzo chiavetta USB), ma anche del controllo dei contenuti (es. tentati accessi ai social network).

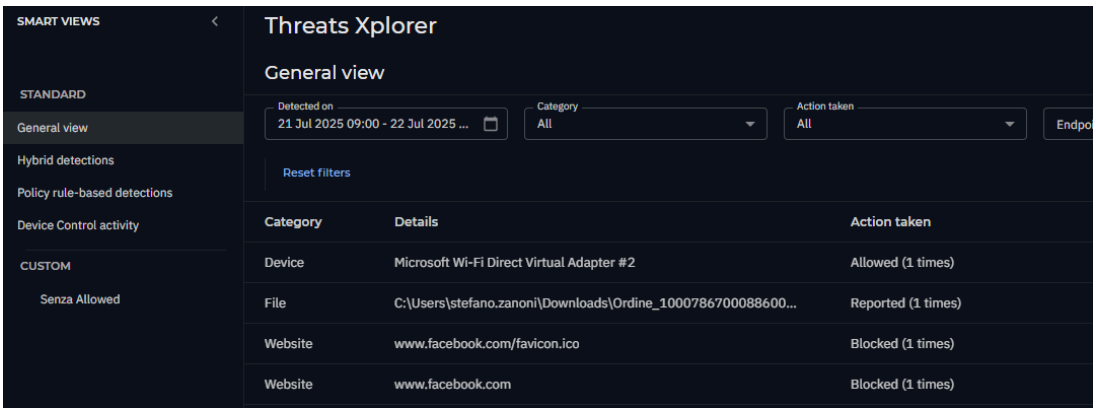

Figure 24: Pagina Threats Explorer

7.7.1. Best Practices

Purtroppo anche inserendoli nelle esclusioni, alcuni “dispositivi” di sistema vengono sempre elencati nella “General View” con stato “Allowed”. È consigliato creare una vista personalizzata rimuovendo i pericoli con stato “Allowed” per maggiore chiarezza visiva.

7.8. Custom Exclusion Rules

Le custom exclusion rules permettono di creare delle eccezioni globali, che una volta attivate saranno applicate a tutti gli endpoint.

Per creare una exclusion rule, andare nella sezione “Incidents -> Custom Exclusion Rules” del menu a sinistra, nella schermata che si apre premere “Add Rule”. Nella finestra che si apre, sarà possibile creare la regola, selezionando la tipologia di controllo da effettuare. Proseguendo con la regola sarà possibile assegnarla a tutti gli endpoint o anche a degli

specifici tag di endpoint, per vedere come gestire i tag, fare riferimento al paragrafo “3 Guida alla gestione dei tag”.

Attenzione, alcuni controllo, basati su tecnologie XDR, non è possibile assegnarli ai tag di endpoint, ma sarà possibile soltanto l’opzione per tutti gli endpoint. La tecnologia che utilizza il controllo scelto è visualizzabile nella prima schermata della regola di esclusione.

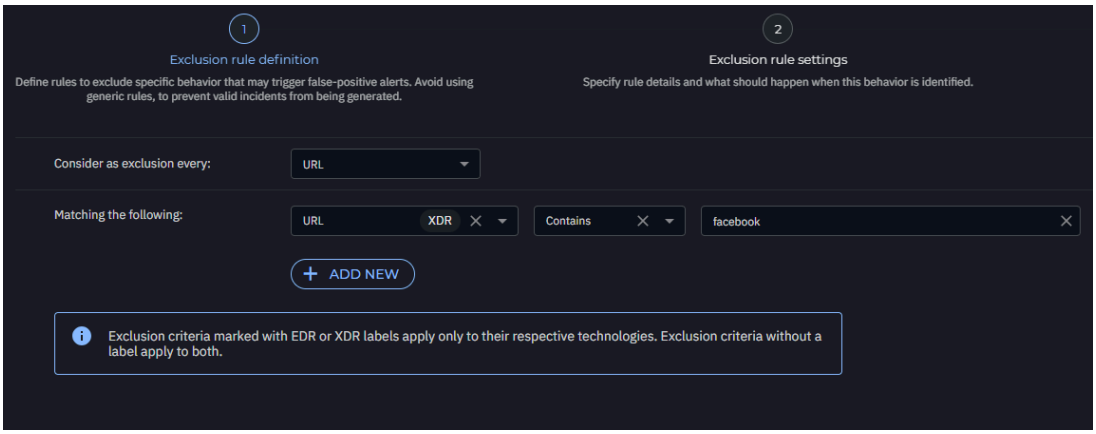

Figure 25: Pagina Threats Explorer