Studio GravityZone

Versione	Data	Redattore	Descrizione
0.6	11/07/2025	Davide Marin	Modifiche al contenuto, aggiunta sezione “Blocklist”
0.5	08/07/2025	Davide Marin	Modifiche al contenuto, aggiunte sezioni del capitolo “Rilevamento”
0.4	25/06/2025	Davide Marin	Stesura sezione “Sicurezza per mobile”
0.3	24/06/2025	Davide Marin	Ampliamento capitolo “Livelli di sicurezza”, in particolare “Controllo Dispositivi”, “Controllo Applicazioni”, “Controllo Contenuti”, “Servizi di test sicurezza”
0.2	20/06/2025	Davide Marin	Inizio stesura capitolo “Livelli di sicurezza”
0.1	19/06/2025	Davide Marin	Inserimento capitolo “GravityZone”

Indice

Lista delle immagini

1. GravityZone

Piattaforma di cybersecurity che gestisce prevenzione, protezione, rilevamento e risposta ad attacchi cyber per aziende di qualsiasi dimensione, comprendendo protezione per server cloud e anche terminali utente, compresi dispositivi mobili.

Dispone di una console dalla quale si può visualizzare la propria esposizione al rischio di attacchi. La console funziona raccogliendo dati da diversi sensori.

Inoltre, è disponibile l'interfaccia "Incident Advisor" che permette di visualizzare le azioni guidate disponibili per risolvere i problemi rilevati da BitDefender.

GravityZone funziona tramite la strategia "Multi-layered Security", che sfrutta AI e Machine Learning per la protezione dagli attacchi.

1.1. Multi-layered Security

Tutte le strategie di protezione valide utilizzano la sicurezza multi-livello, operando sapendo che "nessun sistema è completamente sicuro". La sicurezza multi-livello si suddivide in Prevenzione, Protezione, Rilevamento e Risposta.

Figure 1: Sicurezza multi-livello

Il primo passo è ottimizzare le capacità di prevenzione, identificando e correggendo le vulnerabilità, implementando patch e soluzioni di risk management, prima che gli attori di rischio possano sfruttarle a loro vantaggio.

Il secondo punto è la protezione, tramite GravityZone gli endpoint sono potetti da minacce conosciute e sconosciute. Rilevazione, la rilevazione di minacce avviene con diversi strumenti come i sensori, la Live Search, e gli EDR, XDR, e MDR.

La risposta, infine, permette di investigare sugli incidenti, contenere i pericoli e rimediare ai danni subiti.

1.2. Metodi di Anti-Tampering e Detection Evasion

Gli attaccanti cercano sempre di bypassare gli EDR, questi tentativi si suddividono in due tipologie:

1. Tecniche di disabilitazione diretta: si cerca di disabilitare del tutto il sw di sicurezza (basso livello)

2. Tecniche avanzate di evasione: più sofisticate, di tre diversi tipi
   - **Callback Evasion:** bypassa i messaggi inviati dal sistema al sw di sicurezza dopo determinati eventi
   - **Vulnerabile Drivers:** sfruttano vulnerabilità per ottenere privilegi e poter disabilitare componenti di sicurezza
   - **Event Tracing for Windows:** terminano le sessioni di tracciamento dagli ETW

1.2.1. Mitigazione Callback Evasion

BitDefender prevede la tecnologia CBE (Callback Evasion Detection), che monitora costantemente se alcune callback critiche per la sicurezza subiscono dei tentativi di essere disabilitate. In caso rilevi operazioni sospetta, la CBE genera un alert.

La CBE monitora inoltre se vengono disabilitate le callback dai driver di BitDefender, permettendo di allertare l'utente in caso i driver non siano più in grado di ricevere notifiche di operazioni critiche nel sistema.

1.2.2. Mitigazione Vulnerable Drivers

È presente il BEST (Bitdefender Endpoint Security Tools) agent, esso controlla le applicazioni sconosciute e i driver nel sistema, in cerca di operazioni di driver che cerchino di ottenere accessi non autorizzati. In caso ne trovasse, BEST può disabilitare l'accesso al driver, oppure "disinfettarlo".

1.2.3. Mitigazione Event Tracing for Windows (ETW)

L'ATC (Advanced Threat Control) monitora gli eventuali tentativi di modifica a file come `EtwEventWrite function`, di solito ponendo come prima istruzione return 0 (successo) e quindi così bloccare l'event logging per alcuni eventi. L'ATC può quindi individuare e disabilitare il processo che sta modificando quei file, allertando della cosa l'utente.

1.3. Ottimizzazione di Cloud e Virtualizzazione

BitDefender GravityZone riesce ad essere efficace ed efficiente anche su sistemi cloud o virtualizzati, grazie a integrazioni con tecnologie da Citrix, Nutanix, VMware, e cloud pubblici come Amazon AWS e Microsoft Azure.

2. Livelli di sicurezza

2.1. Prevenzione

2.1.1. Patch Management

Trova bug, errori di configurazione e obsolescenze che possono essere sfruttati per degli attacchi, e li risolve con delle patch.

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 sull’opzione “Patch Scan”, oppure automaticamente creando prima una “Maintenance Window” (selezionando la voce “Configuration profiles” dal menu a sinistra) con le regole desiderate, e poi assegnandola alla policy interessata.

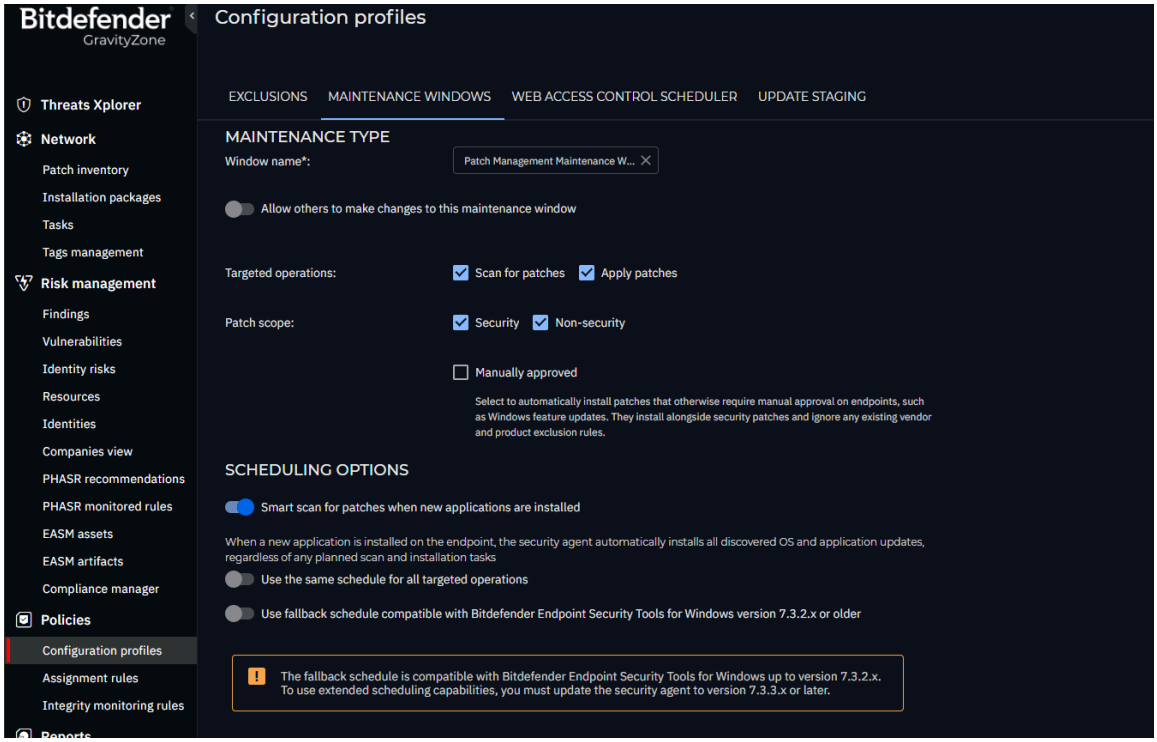

Figure 2: Maintenance Window

2.1.2. Risk Management

2.1.2.1. Cloud (CSPM+)

Per accedere alla configurazione bisogna accedere alla console dedicata.

Il suo scopo non si limita a garantire il rispetto delle compliant per quanto riguarda la configurazione delle risorse in cloud, ma controlla anche che lo IAM (Cloud Identity and Access Management sia rispettato.

Si integra con Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure e Alibaba Cloud.

È importante notare che CSPM+ lavora con i metadata dell'ambiente cloud e non accede a nessun dato, inoltre, si integra direttamente con il provider cloud, e quindi non inficia in nessun modo sul carico di lavoro

2.1.2.2. PHASR

Il PHASR (Proactive Hardening and Attack Surface Reduction), è una tecnologia basata su IA che valuta come ogni individuo interagisce con il proprio sistema e applicazioni, e su questo crea "su misura" dei profili di utilizzo per ogni combinazione macchina-utente (ad esempio un amministratore potrebbe avere un profilo per compiti standard, ed un altro per compiti di amministratore). Per l'adattamento ci vogliono dai 20 ai 60 giorni, se si sta già usando un EDR GravityZone, tramite i dati memorizzati si può portare il processo a qualche minuto.

Il PHASR è utile anche per non dover aver paura di dimenticare qualche privilegio assegnato a un utente, ad esempio nel caso un utente dovesse avere accesso temporaneo alla PowerShell, e ci si dimenticasse di revocarne il privilegio successivamente, il PHASR individuerebbe in automatico la possibilità di toglierlo, in quanto per il comportamento standard dell'utente non è necessario.

Sono disponibili modalità automatica e manuale, nella seconda le modifiche da apportare saranno solo suggerite. Si configura nelle Policies, sotto la voce "Risk Management".

2.1.2.3. Compliance Manager

Il compliance manager permette di visualizzare chiaramente raccomandazioni da seguire per rispettare tutte le norme sulla sicurezza.

È possibile decidere se risolvere un determinato rischio, tramite una procedura guidata, oppure se ignorarlo. Questa operazione nello specifico, è possibile effettuarla anche tramite la schermata "Findings", per avere una panoramica di tutte le macchine, oppure "Resources", per i singoli endpoint, applicando il filtro per la compliance desiderata.

È anche possibile creare report per certificare gli standard di compliance. Questa funzione però, necessita licenze specifiche per ogni tipologia di compliance.

2.1.2.4. Criptazione del disco

È possibile effettuare una criptazione completa del disco e dei dispositivi esterni al pc, sia su Windows che su MacOs che su Linux.

2.1.2.5. Controllo Dispositivi

È possibile creare regole per bloccare un certo tipo di dispositivi (es. chiavette o cd), o dare permessi solo a dispositivi con determinati ID.

Ad esempio, per limitare le USB, selezionare su "External Storage" l'opzione "Custom" e impostare "block" su "USB". Per aggiungere un'eccezione, andare sulla schermata apposita e aggiungere l'eccezione; si potrà inserirla da dispositivi già conosciuti, oppure manualmente tramite ID. Per inserire l'esclusione manualmente, l'ID dell'USB si può trovare in proprietà -> hardware -> proprietà -> eventi -> scorrere il pannello che si visualizza fino alla fine, l'ID è quello segnato in "Dispositivo padre"

2.1.2.6. Controllo Applicazioni

Come per i dispositivi, è possibile limitare l'uso a determinate applicazioni, escludendone altre, impostare regole ed eccezioni.

Si può inserire il percorso esatto, controllando sia corretto e privo di caratteri extra, oppure il nome dell'eseguibile (consigliato)

Si può effettuare il blocco sia all'interno di una policy, sia direttamente nella sezione "Blocklist", che la applicherà quindi a tutti gli endpoint.

2.1.2.6.1. Blocklist

La blocklist permette di bloccare le applicazioni in maniera centralizzata, senza dover creare una policy ad hoc per ogni applicazione da bloccare. Si può accedere alla blocklist dalla sezione "Incidents" -> "Blocklist". Le regole della blocklist però, verranno applicate solo agli endpoint che nella policy hanno abilitato la funzione "Blocklist", e in caso di blocco di un'applicazione, dovranno essere abilitati anche "content control" e "application blocklist" all'interno della policy.

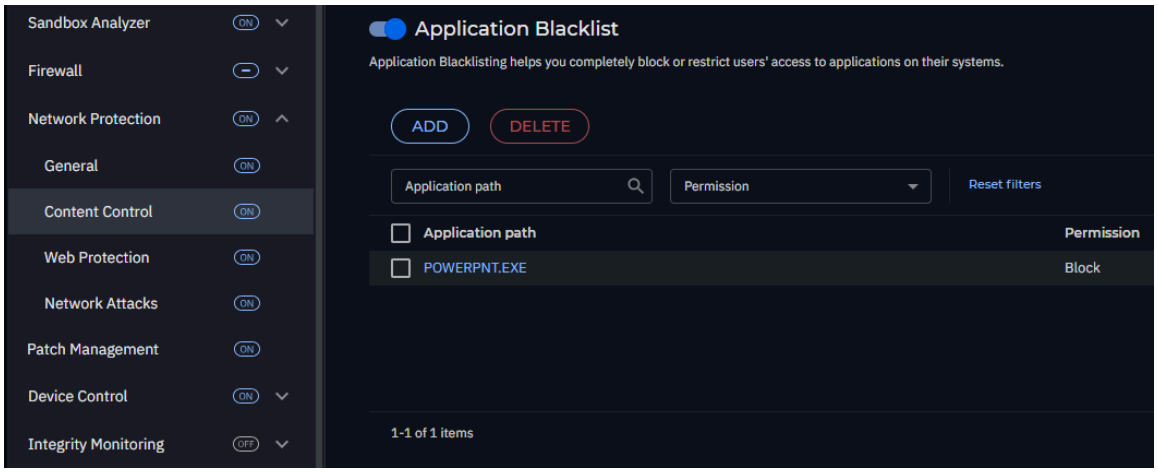

Figure 3: Blocco applicazione da policy

2.1.2.7. Controllo Contenuti

È possibile controllare e limitare l'accesso a determinati contenuti, per motivi di sicurezza, produttività, professionalità ecc. indipendentemente dalla rete in cui ci si trova, utile quindi per lavoro da remoto.

Per il web, prima creare la regola su Configuration profiles -> Web Access Scheduler, poi, andare sulla policy ed assegnare il profilo appena configurato in Network Protection -> Content Control. Infine, ricordarsi di ATTIVARE Intercept Encrypted Traffic in Network Protection -> General.

Per il data protection, sempre all'interno di Network Protection -> Content Control, si possono inserire i dati da proteggere, consigliato è di non inserire interamente dati sensibili, ma magari una loro parte univoca, e selezionare "match case" invece di "hole word" nella parte da scannerizzare.

Di base il controllo avverrebbe solo su HTTP e SMTP, ma con il Intercept Encrypted Traffic attivo, verrà controllato anche il traffico HTTPS.

Per tutti i tipi di controlli è possibile inserire delle esclusioni per i siti fidati, per farlo inserirli nella sezione “Generale”.

2.1.2.8. Servizi di test sicurezza

BitDefender dispone anche di servizi per testare la sicurezza della propria azienda, senza ricorrere in rischi reali, si può fare in maniera automatizzata, oppure tramite ethical hackers. Sono anche disponibili diversi livelli dove si forniscono più o meno dati agli attaccanti per testare le proprie barriere.

Ho comunque provveduto ad effettuare dei test sul antivirus, attraverso “attacchi” file e fileless innocui, i primi tramite la stringa nota di EICAR:

X5O!P%@AP[4PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

I secondi, tramite una simulazione di comportamento fileless su PowerShell, ma con effettuo innocuo, tramite comando:

powershell -nop -w hidden -c “ IEX ‘ Write Output TestFilelessAttack ‘ “

2.2. Protezione

2.2.1. Protezione per E-mail

GravityZone offre diverse opzioni per le e-mail, come filtri anti-spam, anti-malware e filtri in base al contenuto; inoltre permette di creare dei gruppi di utenti, con regole personalizzate per ogni gruppo.

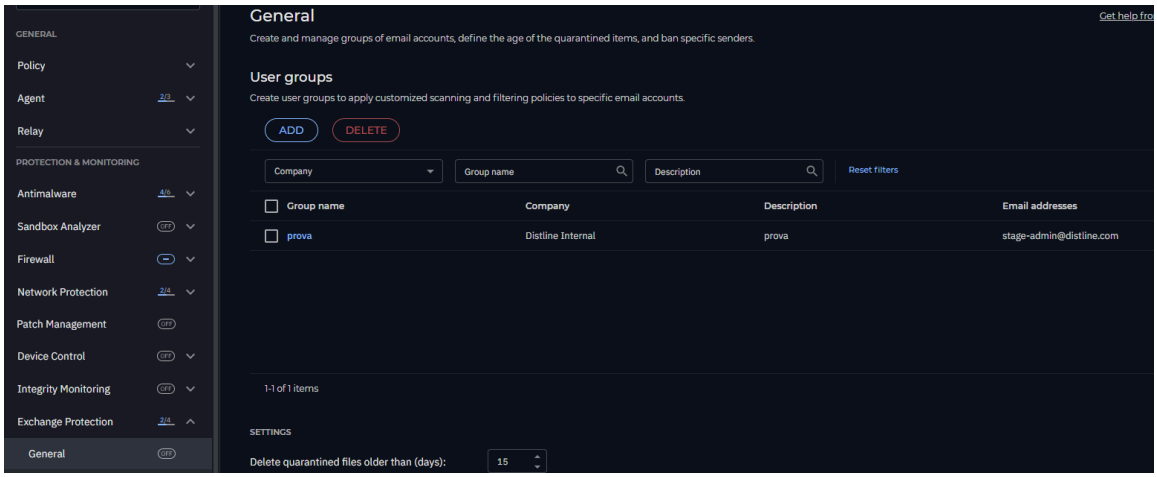

Figure 4: Lista gruppi di e-mail

Nella sezione del filtro per contenuto, è possibile creare regole personalizzate (anche diverse per ogni gruppo di e-mail) sul filtraggio in base ad oggetto, corpo e anche allegati della mail. Attenzione: se si inserisce sia filtro oggetto sia corpo mail, la mail verrà filtrata se almeno una delle espressioni PER TABELLA sarà presente nella mail; quindi, se solo nell'oggetto è presente un match, ma nel corpo no, la mail NON sarà filtrata.

Per la configurazione della protezione mail, però, è necessario licenza e integrazione specifica di Microsoft 365, le aziende potrebbero quindi avere già, o optare per, una soluzione più specifica per le e-mail.

2.2.2. Protezione di rete

Tramite la protezione di rete, è possibile controllare per eventuali pericoli tutto il traffico in entrata e in uscita grazie al Network Attack Defense (NAD). Protezione dai malware Ci sono diversi approcci possibili:

- **Rilevamento e prevenzione:** se impostato rileverà in automatico i pericoli e li bloccherà, cercando la soluzione migliore che può essere disinfettare il file o rimuovere il malware
- **EDR (solo report):** viene abilitato solo il controllo durante l'esecuzione, segnalando ma non bloccando i pericoli trovati, può essere utile in sistemi dove si vuole installare una soluzione EDR leggera. È possibile inoltre impostare il livello di protezione nelle diverse fasi "On-access", "On-Execute" e "On-Demand", l'ultima permette di creare dei task ad esecuzione programmata. La protezione malware di GravityZone si può suddividere in due macro-componenti: "Core" e "Hyper Detect".
  - **Core (di default attivo se è attivo l'anti-malware):** Il sistema può controllare tutti i file locali, può anche estrarre il codice dei vari file e controllarlo per potenziali pericoli.

Dopo l'estrazione, vengono utilizzati emulatori locali per simulare il comportamento del contenuto analizzato, in caso di necessità si passa poi alla disinfezione.

La disinfezione prova dapprima a disinfettare, appunto, il file che risulta infetto, in caso non riuscisse lo sposta invece in quarantena per limitare l'infezione. Per alcuni tipi di malware invece, ad esempio nel caso di file interamente malevoli, essi vengono eliminati direttamente dal disco. Oltre a questo, viene anche controllato se il file ha registrato una chiave per far eseguire il malware all'avvio della macchina, e in caso la chiave viene rimossa

- **Hyper Detect:** è la funzionalità di anti-malware basata su Machine Learning ed è personalizzabile. Tramite questa finestra si possono impostare diversi livelli di aggressività per diverse tipologie di pericoli

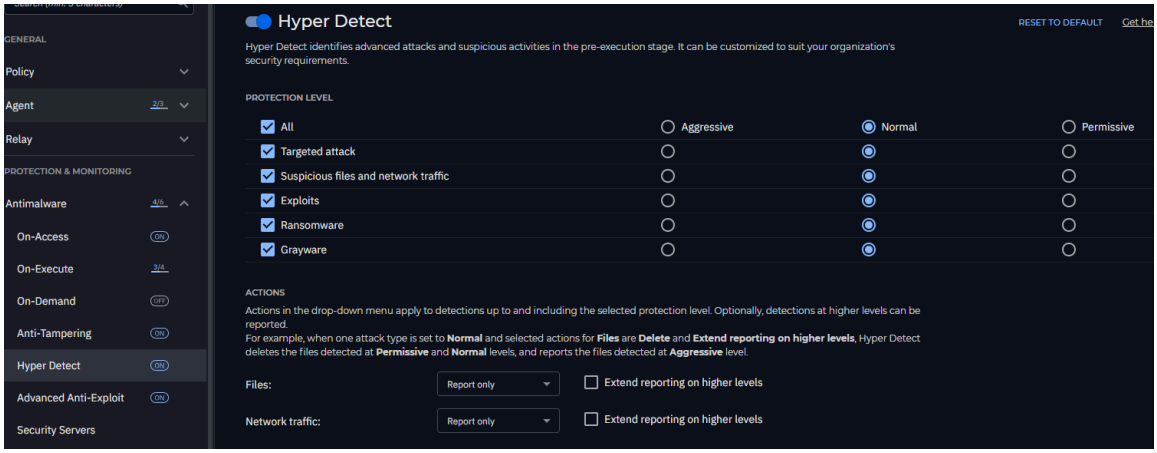

Figure 5: Schermata di Hyper Detect

2.2.3. Protezione dei Processi

La protezione dei processi ha due elementi chiave nel suo funzionamento, ATC e PI:

- **ATC (Advanced Threat Control):** esamina i processi e rileva minacce prima che possano fare danni
- **PI (Process Introspection):** controlla i processi e li ferma nel momento in cui cercano di fare operazioni sensibili non autorizzate

La configurazione per ATP si trova in Antimalware -> On-Execute

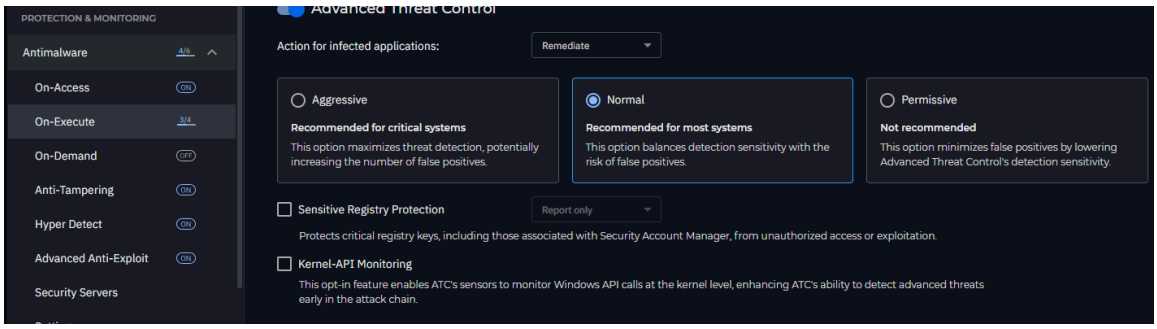

Figure 6: configurazione ATP

2.2.4. Protezione da exploit software

Il modello di Bitdefender controlla i file per potenziali regole o algoritmi associati a tecniche di exploit conosciute, in questo modo riesce a rilevare sia exploit già conosciuti, sia quelli non ancora conosciuti. Il sistema è continuamente aggiornato attingendo a milioni di sensori sparsi in tutto il mondo che continuamente identificano nuove tecniche di exploit e ne migliorano il rilevamento per tutti gli utenti.

La configurazione per exploit si trova in Antimalware -> Advanced Anti-exploit

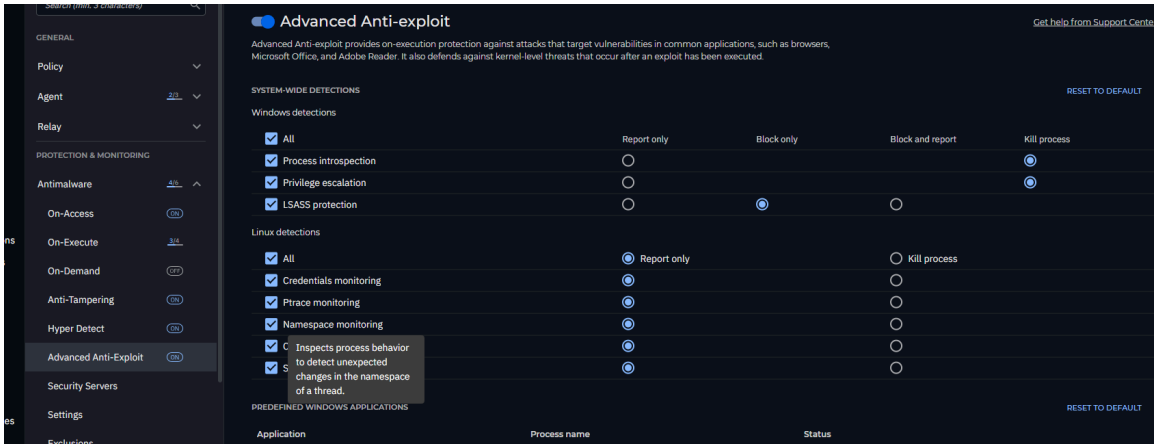

Figure 7: Configurazione Anti-exploit

2.2.5. Protezione da attacchi “fileless”

Gli attacchi fileless sono di tipo Living off the Land.

La protezione da attacchi fileless include due tipi di configurazione: AMSI e Command-Line Scanner.

- **AMSI (Anti Malware Scan Interface):** AMSI lavora come un ponte tra la macchina e GravityZone, e permette di analizzare diversi contenuti (come script, file, URL, ecc.) in cerca di azioni malevole, il tutto prima che il contenuto sia eseguito, riuscendo anche a “de-offuscare” il codice prima di analizzarlo. I suoi punti deboli sono: la compatibilità solo con sistemi con Windows 10 o Windows server 2016 e più recenti, e sistemi con Office 365 aggiornato e con Excel macro-scanning a runtime; e la possibilità di essere bypassato.
- **Command-Line Scanner:** Entra in gioco per rimediare alle mancanze di AMSI, offrendo compatibilità con MacOS, Linux, e versioni di Windows in cui non è disponibile AMSI; inoltre offre sicurezza stratificata, analizzando l’attività su riga di comando e ricercando comportamenti soliti di attacchi fileless. Nello specifico previene l’esecuzione di comandi malevoli.

La configurazione per attacchi fileless si trova in Antimalware -> On-Execute

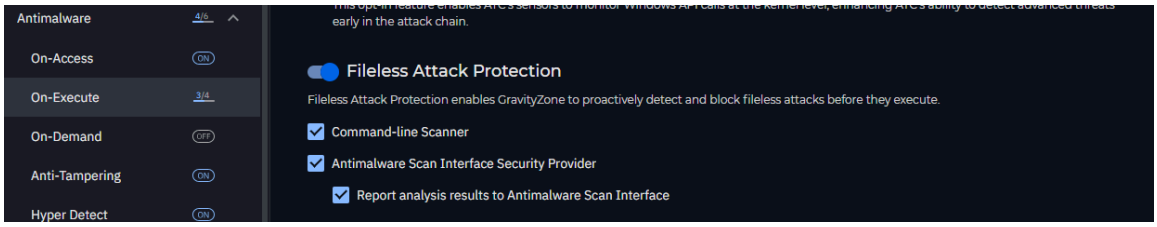

Figure 8: Configurazione Anti-fileless

2.2.6. Sandbox Analyzer

Il servizio di Sandbox utilizza degli ambenti virtuali hostati da Bitdefender per analizzare a fondo i file sospetti. Prima di passare al sandbox, comunque, il file passa per HyperDetect, e in caso servissero ulteriori analisi viene mandato al sandbox. Una volta arrivato 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

La configurazione dell'ambiente sandbox si fa direttamente nella sezione delle policies

2.2.7. Protezione da Ransomware

È presente il modulo di mitigazione per ransomware, nello specifico controlla gli endpoint e blocca operazioni che cercano di alterare i dati senza autorizzazione. Una volta rilevato e bloccato l'attacco, si riceve un report direttamente su GravityZone, che include informazioni su cosa è stato intaccato e opzioni automatizzate e manuali di recupero dati. Attivando la mitigazione da ransomware, si aggiunge uno strato extra di protezione, che comprende tre aree: sistema, file, e cloud.

- **Sistema:** Vengono utilizzati filtri per intercettare la creazione di processi e accessi ai file
- **File:** In caso un'azione su file sembri sospetta, BitDefender fa un backup preventivo, che si può utilizzare per ripristinare il file, in maniera manuale o automatica, se la minaccia si rivelasse reale

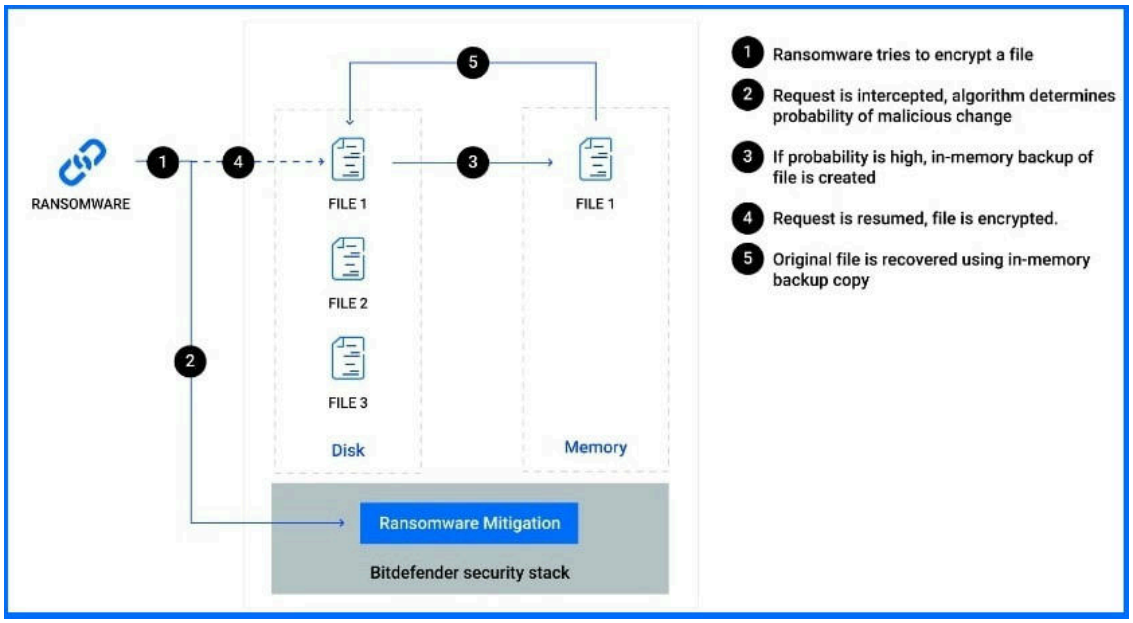

Figure 9: Funzionamento mitigazione per file

- **Cloud:** Il servizio cloud è utile per testare i nuovi algoritmi di ransomware, nonché per mitigare velocemente il rilevamento di falsi positivi e negativi.

La configurazione della mitigazione per ransomware si trova sempre in Antimalware -> On-Execute

Sicurezza per mobile Ci sono diverse tipologie di soluzioni per la sicurezza mobile:

- **MDM (Mobile Device Management):** controlla le impostazioni di sistema, stato del dispositivo, distribuisce applicazioni e può anche disinstallarle e fare altre operazioni da remoto.
- **MAM (Mobile Application Management):** si concentra prettamente sul controllo delle applicazioni. È meno invasivo del MDM dal punto di vista della privacy.
- **EMM (Enterprise Mobility Management):** è la fusione di MDM e MAM in un'unica piattaforma.
- **UEM (Unified Endpoint Management):** fa un passo avanti rispetto agli EMM, si applica infatti a tutti i dispositivi e non solo ai mobili.
- **MTD (Mobile Threat Defense):** soluzione che è pensata per proteggere i dispositivi mobili da attacchi cyber.

BitDefender offre una combinazione di MDM e MTD, in quanto possono lavorare assieme.

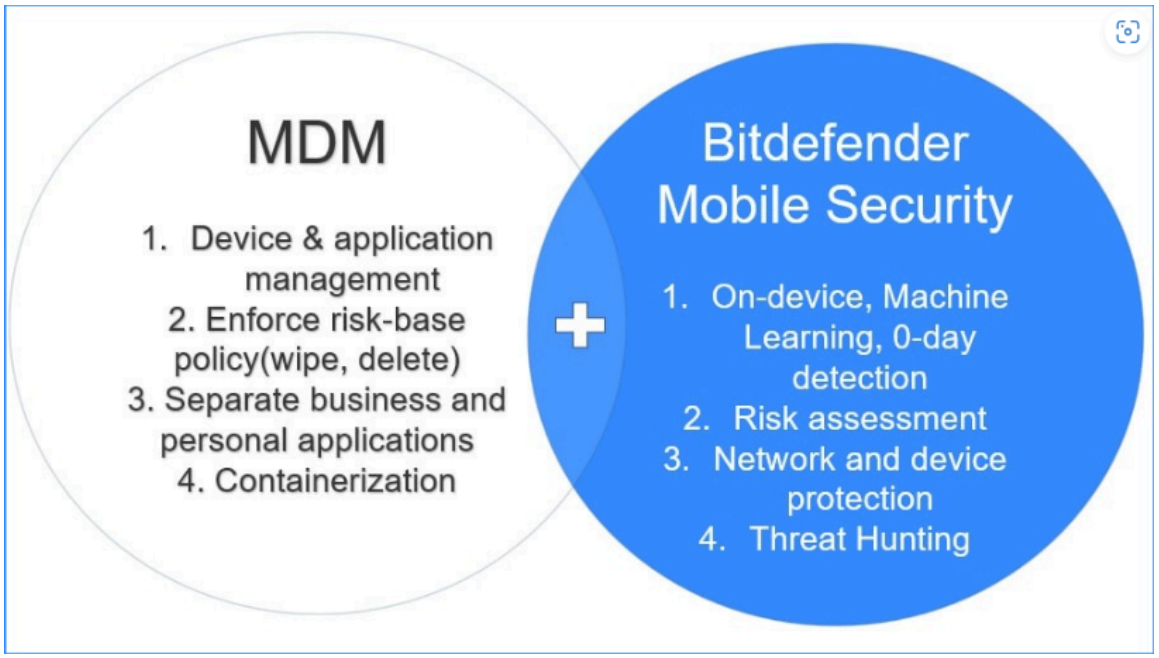

Figure 10: Combinazione MTD con MDM

2.3. Rilevamento

2.3.1. Sensori

I sensori di GravityZone monitorano attivamente i dispositivi, il cloud ecc., per potenziali pericoli, compresi i ransomware.

2.3.2. EDR, XDR, e MDR

Tutto parte dagli EPP (Endpoint Protection Platform), sono l'evoluzione degli antivirus, che incorporano multipli layer di sicurezza e tecnologie come l'Advanced Machine Learning. Gli EDR (Endpoint Detection and Response) utilizzano le funzionalità degli EPP, estendendone la visibilità prendendo dati da tutti gli endpoint. Sono tenuti sotto controllo anche i lateral movement nella rete, ad esempio se un utente inserisce dei dati in una nuova macchina che risulta corrotta, verrà visualizzato come utente a rischio, e saranno quindi indicate le altre macchine sul quale ha effettuato l'accesso come a rischio.

Gli XDR (Extended Detection and Response) invece, vanno oltre al funzionamento degli EDR, estendendo il numero e il tipo di sensori dai quali possono recuperare dati.

2.3.3. Investigazione degli incidenti

La pagina "Incidents" permette di visualizzare tutti gli incidenti rilevati e le azioni che sono state prese in automatico e quelle consigliate da BitDefender per risolvere i problemi. Inoltre, sono presenti schermate di investigazione più o meno dettagliate e tecniche per mostrare i possibili rischi individuati:

- **Incident Advisor:** Semplici informazioni mostrate in una singola pagina
- **Graph:** Visualizza un grafico rappresentante la progressione dell'attacco rilevato
- **Alerts:** Visualizza il flusso dettagliato e relazioni tra processi e operazioni del file system

Attraverso l'investigazione GravityZone suggerisce le azioni da intraprendere per risolvere i problemi.

2.3.4. Live Search

A disposizione dell'utente c'è ache la Live Search (che per essere utilizzata deve essere prima attivata nella policy degli endpoint interessati), che permette di effettuare ricerche, tramite query "SQL-like", in tempo reale sugli endpoint per reperire diverse informazioni. Questa funzionalità si rivela utile nel caso si riscontrassero degli attacchi, per monitorare lo stato della rete e dei dispositivi in tempo reale, per capire al meglio come intervenire.

2.4. Risposta

2.4.1. Threat Response

Bitdefender offre diverse opzioni di risposta in caso di attacchi subiti, se le operazioni di protezione non fossero bastate. Dalla pagina degli incidenti è infatti possibile visualizzare le azioni consigliate (isolare endpoint, mettere in quarantena il file, ecc.) per ogni incidente. È disponibile anche una pagina dedicata, chiamata "Response" disponibile nel dettaglio degli incidenti, qui è possibile visualizzare le operazioni da intraprendere sotto forma di lista.

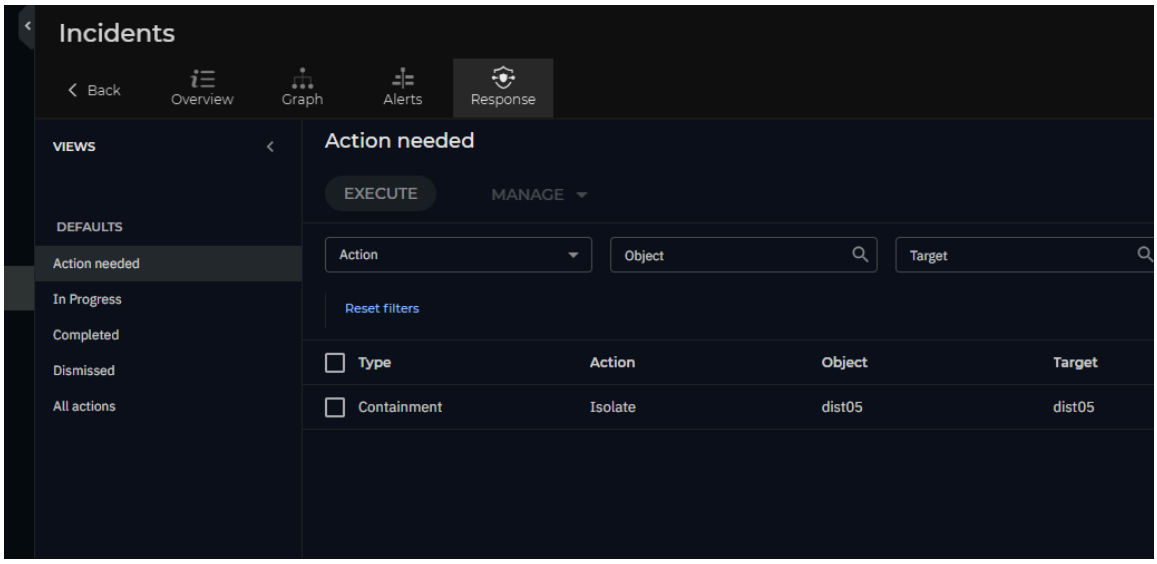

Figure 11: Lista operazioni consigliate