

Bitdefender®

端點偵測及回應(EDR)

# 擴展的威脅偵測、深度調查及有效的回應



# 您今天面對的進階威脅挑戰

網路犯罪份子越來越複雜，進階攻擊越來越難以發現。使用單獨看起來像是常規行為的技術，攻擊者可以進入您的基礎架構並持續數個月都不被發現，這大幅增加了代價慘重的數據洩漏風險。

## Bitdefender 端點偵測及回應(EDR)如何幫忙呢？

當您現有的端點安全無法提供進階攻擊所需的可視性和回應能力時，選擇易於使用的Bitdefender端點偵測及回應(EDR)，可快速有效地強化您的安全操作。

### 擴展的攻擊偵測與回應

Bitdefender EDR監控您的網路以儘早發現網路中的可疑活動，並提供擊退網路攻擊的工具。

- 強化的威脅偵測與可視性，可發揮XDR\*的優勢以保護端點。
- EDR整合了Bitdefender獲獎的機器學習、雲端掃描和沙箱分析器，以偵測逃避傳統端點保護機制的活動。
- 全方位搜尋功能可以針對特定入侵指標(IOC)、MITRE ATT&CK技術，及其他痕跡鑑識，以發現早期的攻擊。[2021年4月份的MITRE ATT&CK 評測中](#)，Bitdefender在整個攻擊鏈的每個步驟中提供了可採取行動的偵測和警報，表現出色。
- 採取回應措施以關閉漏洞並消除重複攻擊的風險。

### 縮小網路安全技能的差距

- 易於遵循的內建回應工作流程讓您的團隊能夠有效地回應，限制橫向擴散並阻止進行中的攻擊。
- 具有一鍵解決功能的自動警報優先級分類。

### 降低組織風險\*

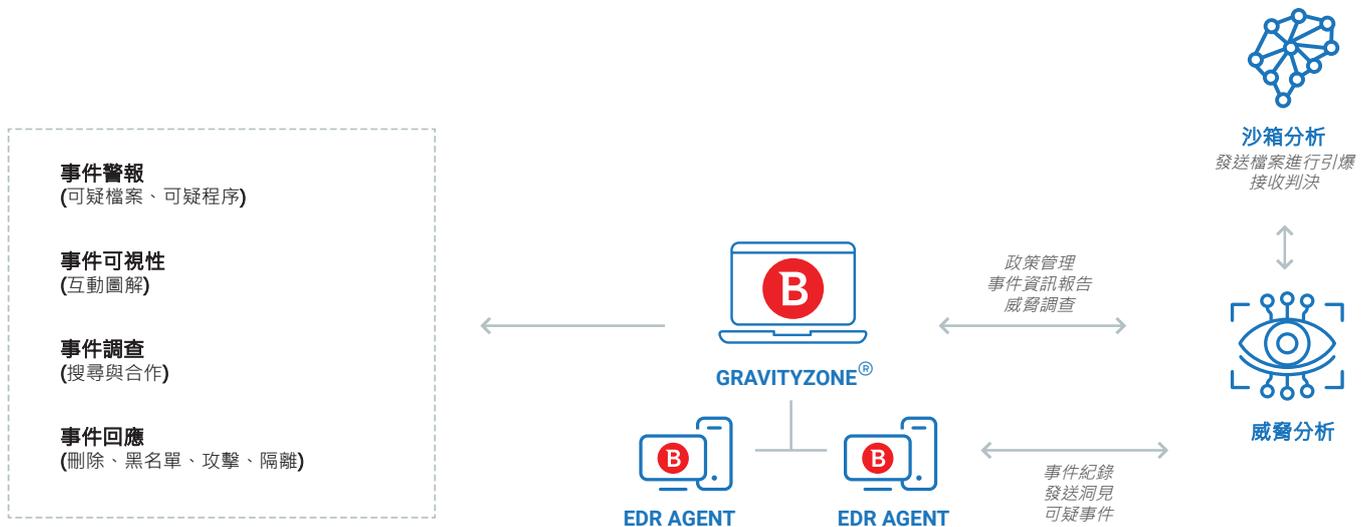
- EDR利用獨特的功能持續分析您的組織，以辨識數百種因素中的風險。它提供了明確的指引，以幫助您減輕用戶、網路和操作系統的風險。

### 減少營運負擔

- EDR可作為雲端與本地的託管解決方案。易於部署，並整合到您現有的安全體系架構中，且與您當前的端點防毒解決方案完全兼容。
- 輕量級Agent具有較低的硬碟空間、記憶體、頻寬和CPU資源開銷。
- 靈活、可擴展與可升級至完整的Bitdefender端點防護平台以及託管式偵測及回應(MDR)。

\* 僅限雲端交付的解決方案

# 如何運作



上圖：Bitdefender端點偵測及回應

Bitdefender EDR是建立於Bitdefender GravityZone雲端平台的雲端或本地託管解決方案。EDR Agent會部署在您組織的端點上。每個EDR Agent都有一個事件紀錄器持續的監控端點，並將洞見與可疑事件安全地發送到GravityZone雲端。

在GravityZone，威脅分析模組收集端點事件並將其提取到事件的優先級列表中，以進行額外的調查及回應。在沙箱分析器中發送可疑檔案進行引爆，然後在EDR的事件報告中使用沙箱判決。可以從任何設備存取EDR即時儀表板，使管理者可以查看警報與可視性，然後對威脅進行有效調查及回應。

# Bitdefender端點偵測及回應(EDR)特點

## 風險分析\*\*

### 人力以及端點風險分析

利用數百種因素持續分析組織中風險，以識別、優先級順序化並為減輕使用者、網路、端點風險提供指引。利用數百種因素持續分析組織中風險，以識別、優先級順序化並為減輕使用者、網路、端點風險提供指引。

## 偵測

### 擴展的端點偵測及回應(XEDR)\*\*

這種跨端點相關技術通過應用XDR功能，偵測涉及混和基礎架構(工作站、伺服器或容器、運作各種作業系統)中的多個端點的進階攻擊，將威脅偵測及可視性提升到新的水平。

### 威脅分析

基於雲端的事件收集器不斷將端點事件分發到事件優先級列表中，以進行事件調查及回應。

### 事件記錄器

持續監測端點事件，將事件反饋給威脅分析，以構建攻擊中的事件帶來的威脅可視性。

### 沙箱分析器

在虛擬容器中自動執行可疑的payloads。然後，威脅分析模組利用此分析對可疑檔案做出決策。

## 調查及回應

### IoC 查詢

查詢事件資料庫以發現威脅。揭示攻擊者採用MITRE ATT&CK技術和入侵指標。即時了解偵測的威脅和可能涉及的其他惡意軟體。

### 組織層面的攻擊可視性

全面且易於理解的將對手行為可視性，結合了上下文和威脅情報，凸顯了關鍵的攻擊途徑，減輕IT工作人員負擔。幫助識別保護和事件影響方面的差距，以支持合規性。

### 引爆

操作者發起的沙箱調查可幫助您對可疑檔案做出明智的決策。

### 黑名單

將EDR偵測到的可疑檔案或程序阻止運行，避免傳播到其他機器。

\*\* 僅限雲端交付的解決方案



## 終止程序

立刻結束可疑程序，以阻止潛在的實時破壞

## 網路隔離

在調查事件時，阻止端點連接網路，以防止橫向移動和進一步的破壞

## 遠端shell連接

在任何工作站上執行遠端指令，以對正在發生的事件立即作出反應

# 報表與警報

## 儀表板和報告

可配置的儀表板與全面的即時和計劃報告功能

## 通知

可配置的儀表板和電子郵件通知

## 結合SIEM與API支援

支援與第三方工具的進一步整合

# 績效與管理

## 優化的EDR Agent

CPU、RAM、硬碟空間使用率低

## Web控制台

易於使用的雲端託付管理

# 關於 Bitdefender

Bitdefender是網路安全領導者，於全世界提供一流的威脅預防、偵測及回應解決方案。守護數百萬的客戶、企業和政府環境，Bitdefender是業界受信賴\*的消除威脅、保護隱私與數據，以及實現網路彈性的專家。Bitdefender Labs對研究與開發投入了大量的投資，每分鐘發現400個新威脅，並且每天驗證300億個威脅查詢。該公司在反惡意軟體、物聯網安全、行為分析和人工智能開創了突破性的創新，其技術被超過150個全球最知名的技術品牌授權。成立於2001，Bitdefender的客戶遍及170個國家且於世界各地設有辦事處。

排名 #1 的資安。榮獲全球獎項。



想知道更多資訊以及其他Bitdefender的產品及服務，請至

<http://www.cyberview.com.tw/bitdefender-2/>



力悅資訊股份有限公司

■ 台北市中山區松江路54號4F-4 ■ 02-25429758 ■ Sales@cyberview.com.tw

\*Bitdefender has ranked #1 in 54% of all tests by AV-Comparatives 2018-2021 for real-world protection, performance, malware protection & advanced threat protection.

All Rights Reserved. © 2021 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners.

## Bitdefender

### UNDER THE SIGN OF THE WOLF

Founded 2001, Romania  
Number of employees 1800+

Headquarters  
Enterprise HQ – Santa Clara, CA, United States  
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES  
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA  
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS  
Australia: Sydney, Melbourne

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win – a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.