DATASHEET

Bitdefender

端點偵測及回應(EDR)

進階威脅偵測、深度調查及有效的回應

www.bitdefender.com

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。

進階的攻擊偵測與回應

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。

- 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。
- 全方位可視性用於攻擊系統的技術、戰略和程序(TTPs)。
- 全方位搜尋功能可以針對特定入侵指標(IOCs) 、MITRE ATT&CK技術，及其他痕跡鑑識，以發現早期的攻擊。2020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

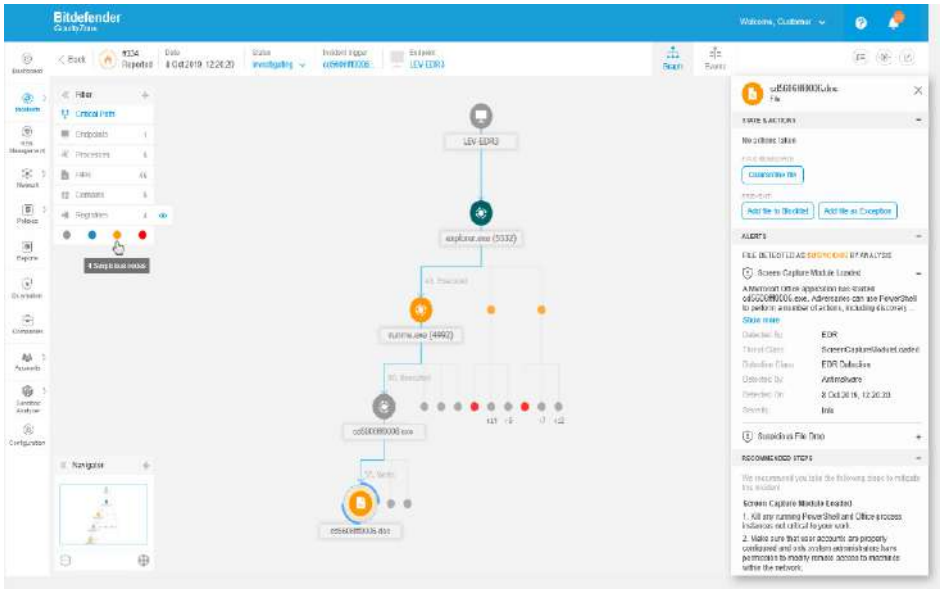
- 易於遵循的內建回應工作流程讓您的團隊能夠有效地回應，限制橫向擴散並阻止進行中的攻擊。
- 威脅可視性幫助您可以專注進行事件調查，了解攻擊複雜的偵測，找出攻擊的根本原因並讓您的直接回應能力最大化。
- 具有一鍵解決功能的自動警報優先級分類。

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

- 雲端提供且維護成本低，EDR易於部署，並整合到您現有的安全體系架構中，且可與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)。

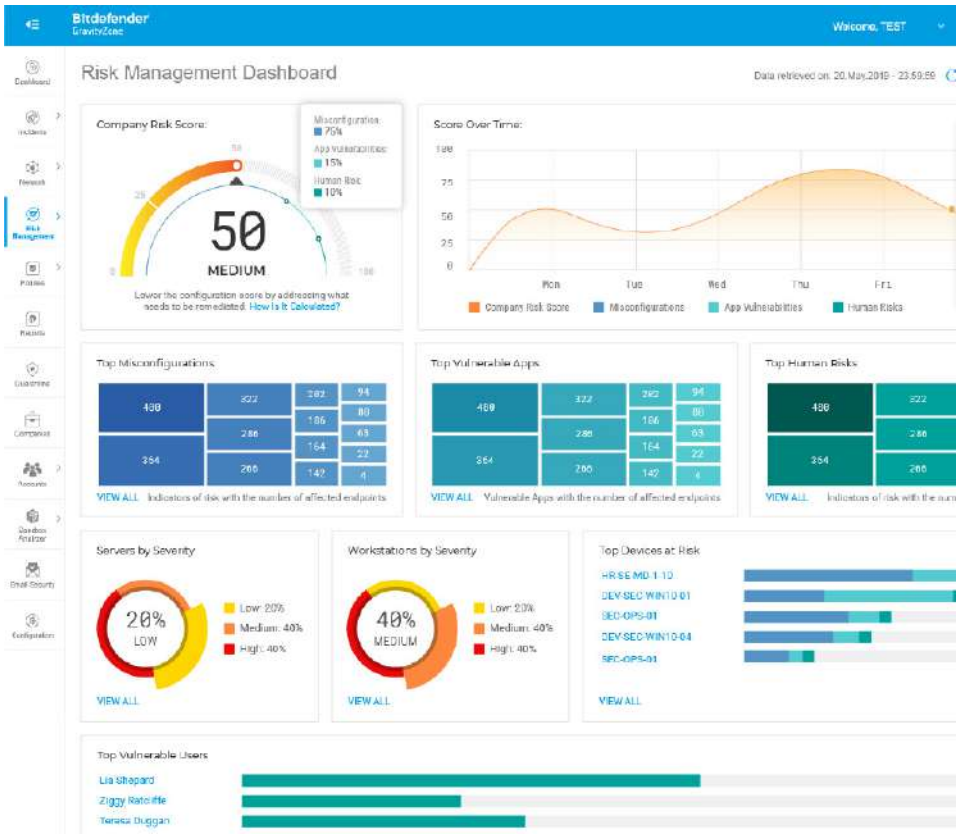


進階的偵測與回應功能可精確顯示潛在威脅的工作方式及您環境中的威脅情況。
MITRE攻擊技術及入侵指標可提供有關命名威脅及其他可能涉及的惡意軟體的最新見解。
易於理解的視覺化指南強調關鍵的攻擊路徑，減輕IT人員的負擔。

用於連續攻擊面管理的端點及使用者行為風險分析

於整個企業範圍內啟用Active System強化程序

Bitdefender的端點風險分析(ERA)引擎使組織能夠通過易於理解的優先級列表，持續評估，識別優先級並強化端點安全性錯誤配置和設定。憑藉其獨特的端點和使用者行為風險分析讓GravityZone可以不間斷地減少攻擊面。



GravityZone Ultra風險管理儀表板。查看貴公司整體的風險分數，並了解各種錯誤配置、應用程式漏洞和人員行為如何影響該錯誤評分。

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

偵測

世界頂級的偵測技術

即時偵測進階威脅，包括無檔案型態攻擊、勒索軟體，以及其他零時差威脅。對您現有的端點安全解決方案進行補充，以強化偵測能力

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

攻擊可視性

易於理解的視覺指引，結合了上下文和威脅情報，凸顯了關鍵的攻擊途徑，減輕IT人員的負擔。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

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

為什麼選擇Bitdefender

無庸置疑的創新領導者。
全球超過38%的網路安全供應商使用Bitdefender技術。Bitdefender為全球網路安全領域的領導者，在150多個國家/地區保護著5億個系統。

全球第1個端到端的洩漏避免
第一個橫跨端點、網路及雲端的統一強化、預防、偵測與回應之安全解決方案。

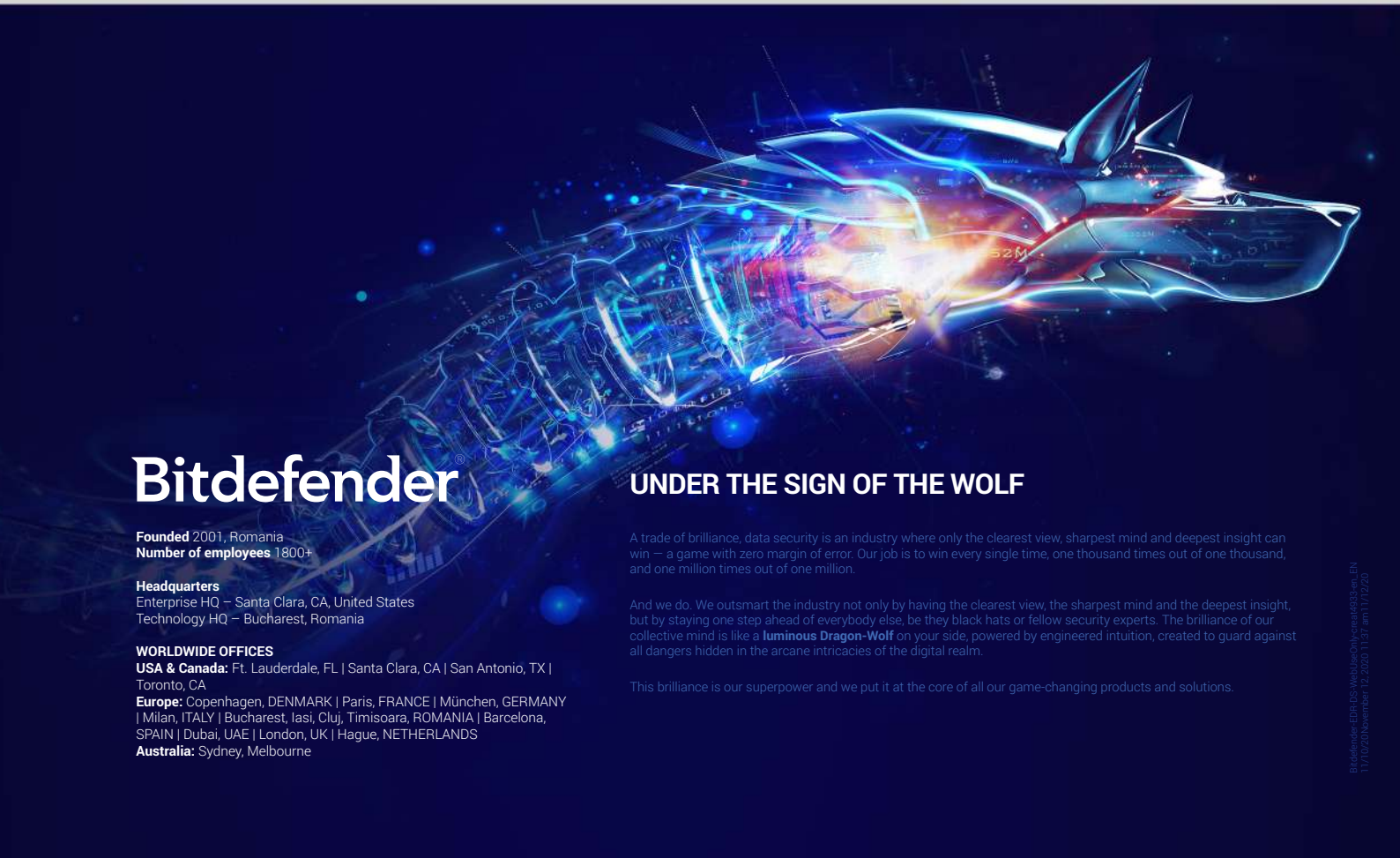
排名＃1的資安。榮獲全球獎項。

想知道更多Endpoint Detection and Response細節以及其他Bitdefender的產品及服務，請至
http://www.cyberview.com.tw/bitdefender-2/

Bitdefender

Cyberview 力悅資訊

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

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

UNDER THE SIGN OF THE WOLF

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.

Bitdefender-EDR-DS-WebUseOnly-creat4503-en_EN
11/10/20November 12, 2020 11:37 am11/12/20