端點防護最完整方案
相見恨晚

端點 ● 網路 ● 雲端

Bitdefender台灣代理商 力悅資訊 彭國達

Bitdefender

WWW.BITDEFENDER.COM

Cyberview 力悅資訊

簡報大綱

- 簡介
- 得獎
- 效益
- 功能
- 端點、網路
- 產品組合
- 部份產品功能展示

Bitdefender: 全球性 資訊安全創新者

We provide: end-to-end breach avoidance
@endpoint @network @cloud

創立於：2001

專業的技術研發公司

超過150家的資安供應商使用
Bitdefender技術

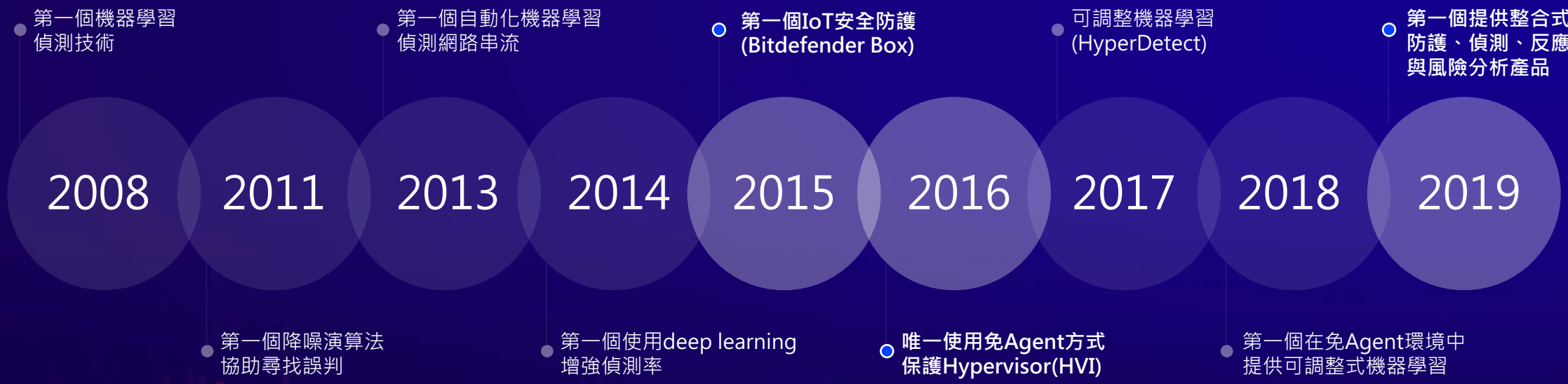
全球最大sensor網路
超過五億個設備

ENTERPRISE HQ IN BUCHAREST, ROMANIA AND BRANCH OFFICES IN US, UK,
EUROPE, MIDDLE EAST, AUSTRALIA

Cyberview 力悦資訊

業界公認技術創新的領先者

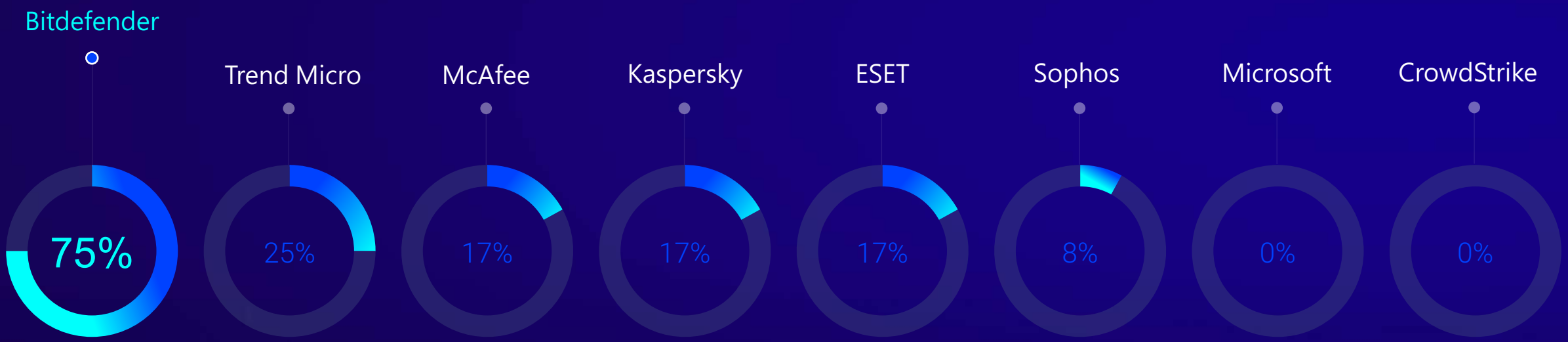
專利得獎技術為38%的資安供應商採用



PATENT PORTFOLIO: 48 GRANTED, 28 PENDING. MACHINE-LEARNING PIONEER SINCE 2008.

無可匹敵的攻擊防禦能力

2018 & 2019 AV comparatives公正第三方測式中，獲得最多 #1 排名



BASED ON ENTERPRISE AV COMPARATIVES RESULTS FROM JAN 2018 UP TO SEP 2019 (REAL-WORLD PROTECTION, PERFORMANCE & MALWARE PROTECTION TESTS).

全球第三方資安分析 & 評測單位公認

"Bitdefender贏得"年度產品"大獎，並在2019年七項測試中獲得Advanced+高分成績

AV-Comparatives
進階實戰測試中達成
100% 偵測率

"企業用戶最佳產品" AV-Test

Leader in the inaugural Forrester® WAVE ™ for Cloud Workload Security

Strong Performer in *Forrester® WAVE for Enterprise Detection and Response*

Gartner has once again included Bitdefender in the 2019 Magic Quadrant for Endpoint Protection Platforms for its GravityZone Ultra product

"Received a score of 100% for evasions. No false positives" NSS Labs

"5/5"
"WEAKNESSES: None that we found."

TRUSTED BY
ENTERPRISES AND LAW ENFORCEMENT AGENCIES

RELIED ON
in key technology partnerships

PARTNERED & PROTECTING KEY ORGANIZATIONS WORLDWIDE

Mentor A Siemens Business
TUI
Commerce State Bank
Speedway Motorsports, Inc.
esurance
YAMAHA
Honeywell

amazon web services Partner Network TECHNOLOGY PARTNER
CITRIX PARTNER Citrix Ready
NUTANIX READY INTEGRATED
Microsoft Partner
vmware READY NETWORKING AND SECURITY
Pivotal PIVOTAL TECHNOLOGY PARTNER PREMIER

PARTNERING AGAINST CYBER CRIME

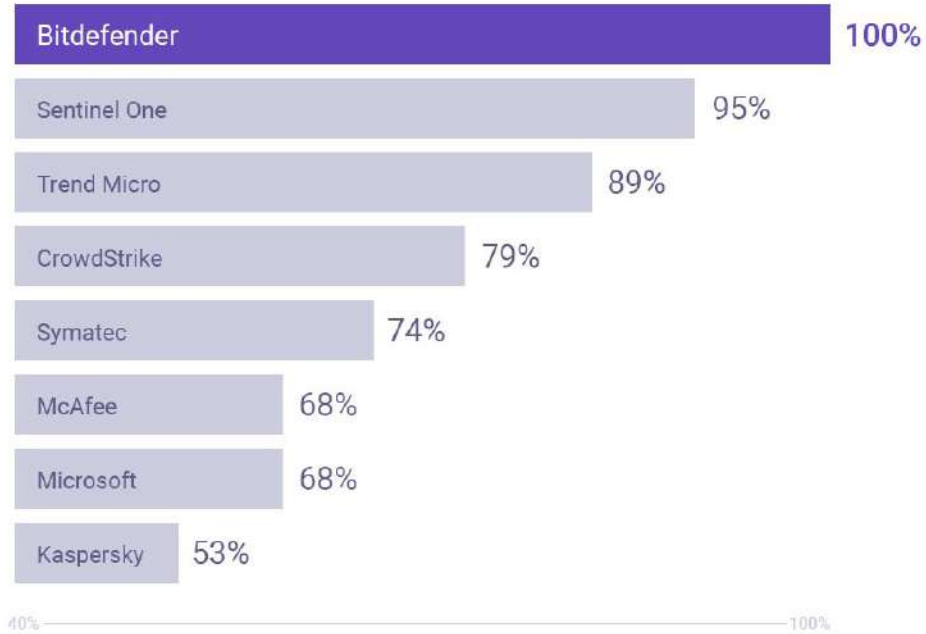
FBI
Department of Justice
EUROPOL EUROPEAN LAW ENFORCEMENT AGENCY

TRUSTED BY

100%
涵括MITRE ATP29攻擊手法
Apr 2020

Complete MITRE ATT&CK Coverage

for mid-sized organisations & MSPs

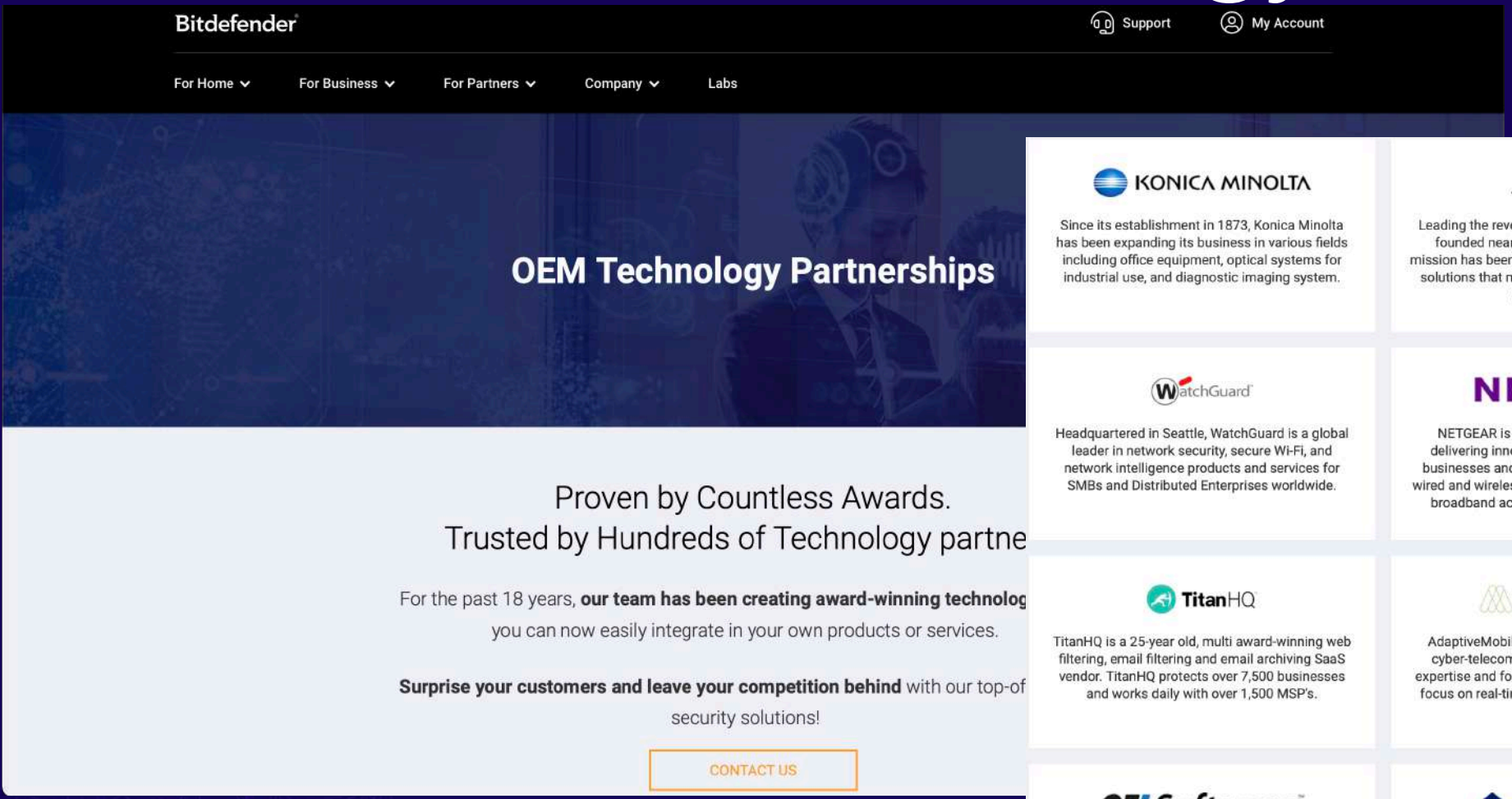


Bitdefender reaches 100% coverage after completing all 19 attack chain steps defined in the MITRE ATT&CK round 2 evaluation of APT29. Apr 2020
This chart analyzes coverage of techniques, tactis and general detection, the most relevant ones for mid-sized organisations and MSPs, that are looking for processed EDR data.
For more info: https://attackevals.mitre.org/APT29/results/bitdefender/

MITRE | ATT&CK®

GRAVITYZONE™
THE SECURITY PLATFORM FOR
END-TO-END BREACH AVOIDANCE

OEM Technology Partnerships



KONICA MINOLTA

Since its establishment in 1873, Konica Minolta has been expanding its business in various fields including office equipment, optical systems for industrial use, and diagnostic imaging system.

JUNIPER NETWORKS

Leading the revolution in networking, since being founded nearly 20 years ago, Juniper's sole mission has been to create innovative products and solutions that meet the growing demands of the connected world.

FIREEYE

FireEye is the leader in intelligence-led security-as-a-service. It offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting.

WatchGuard

Headquartered in Seattle, WatchGuard is a global leader in network security, secure Wi-Fi, and network intelligence products and services for SMBs and Distributed Enterprises worldwide.

NETGEAR

NETGEAR is a global networking company delivering innovative products to consumers, businesses and service providers, consisting of wired and wireless devices that enable networking, broadband access and network connectivity.

Acronis

Founded 2003, Acronis sets the standard for cyber protection through its innovative backup, anti-ransomware, disaster recovery, storage, and enterprise file sync and share solutions.

TitanHQ

TitanHQ is a 25-year old, multi award-winning web filtering, email filtering and email archiving SaaS vendor. TitanHQ protects over 7,500 businesses and works daily with over 1,500 MSP's.

adaptivemobile

AdaptiveMobile Security is the world leader in cyber-telecoms security, powered by its core expertise and foundation in security with a unique focus on real-time mobile network enforcement.

LogMeIn

LogMeIn simplifies how people connect with each other and the world around them to drive meaningful interactions, deepen relationships, and create better outcomes for individuals and businesses.

GFI Software

GFI develops right-sized, smartly engineered IT solutions, enabling IT administrators to efficiently discover, manage and secure their business networks, systems, applications and communications wherever they exist.

KERIO

Part of the GFI Software family, Kerio provides award-winning email, UTM/firewall, VoIP, and collaboration solutions to more than 60,000 businesses and millions of users globally.

endian

Endian is a leading security manufacturer in the field of Industry 4.0. The product range extends from security solutions for SMBs over hotspot management to solutions for industrial production plants.

資料來源：https://www.bitdefender.com/oem/technology-partnerships.html

Bitdefender

“Bitdefender 最受到客戶重視的是單一Agent，單一管理平台就可為所有企業設備提供完整保護”

Gartner®

Cyberview 力悅資訊

WHY BITDEFENDER

38%

領先的技術提供者，
38%以上的資安供應使用
Bitdefender整合

BEST PREVENTION

無可比擬的攻擊防護.
第三方評測長期#1

INTEGRATED PLATFORM

第一個整合式平台完整保護
端點、網點、手持、IoT、雲端

企業等級資安平台

單一平台&Agent為所有端點、網路與需端
提供預防、偵測、反應與強化

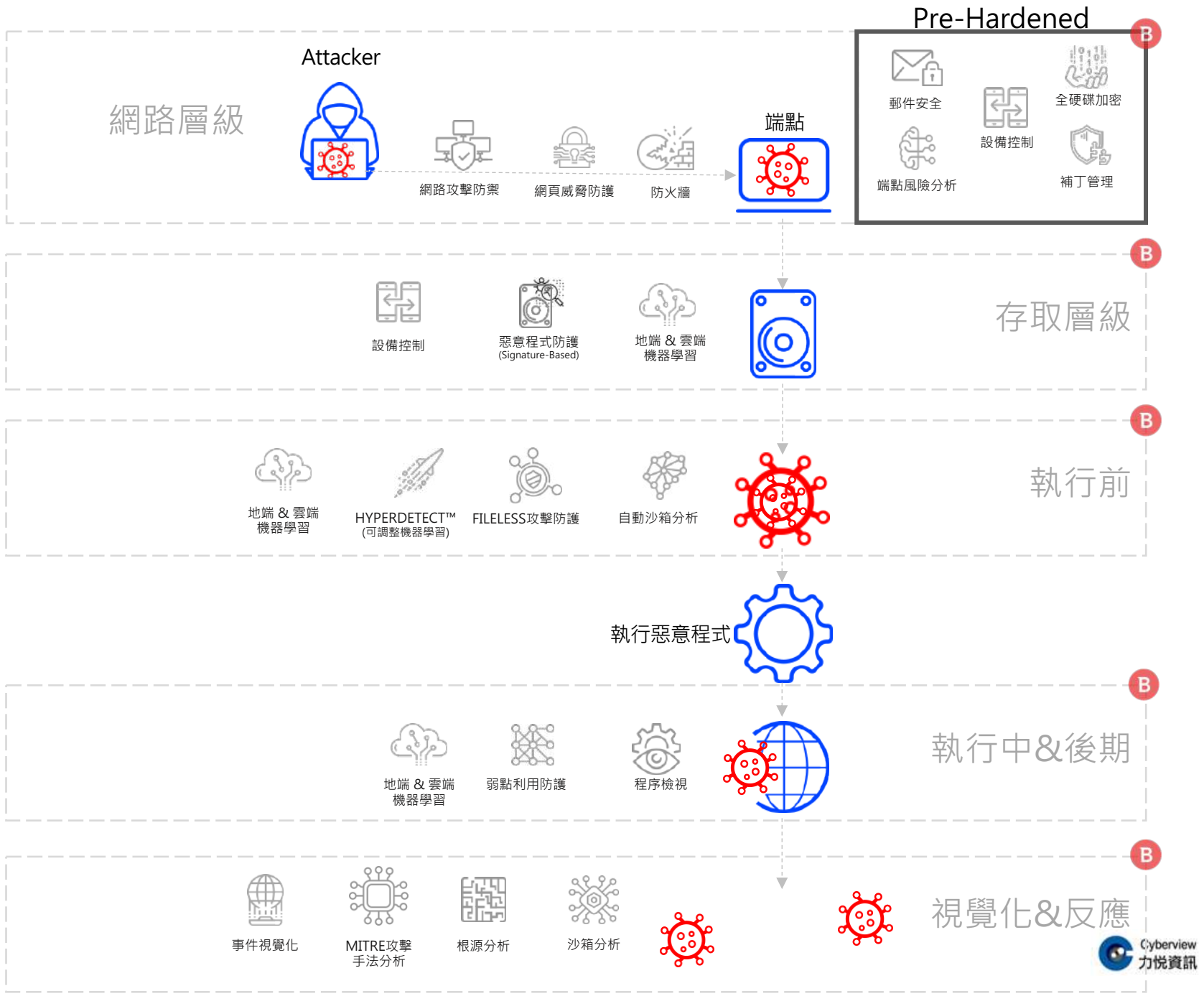
整合
技術 & 服務
提供最佳防護

Bitdefender GravityZone
次世代安全平台
保護企業內所有的端點
包括用戶設備
虛擬、實體基礎設施

BITDEFENDER GRAVITYZONE®

@端點

最佳多層次保護


Pre-Hardened
Attacker
網路層級
端點
網路攻擊防禦
網頁威脅防護
防火牆
郵件安全
全硬碟加密
設備控制
端點風險分析
補丁管理
存取層級
設備控制
惡意程式防護
(Signature-Based)
地端 & 雲端
機器學習
執行前
地端 & 雲端
機器學習
HYPERDETECT™
(可調整機器學習)
FILELESS攻擊防護
自動沙箱分析
執行惡意程式
執行中&後期
地端 & 雲端
機器學習
弱點利用防護
程序檢視
視覺化&反應
事件視覺化
MITRE攻擊
手法分析
根源分析
沙箱分析

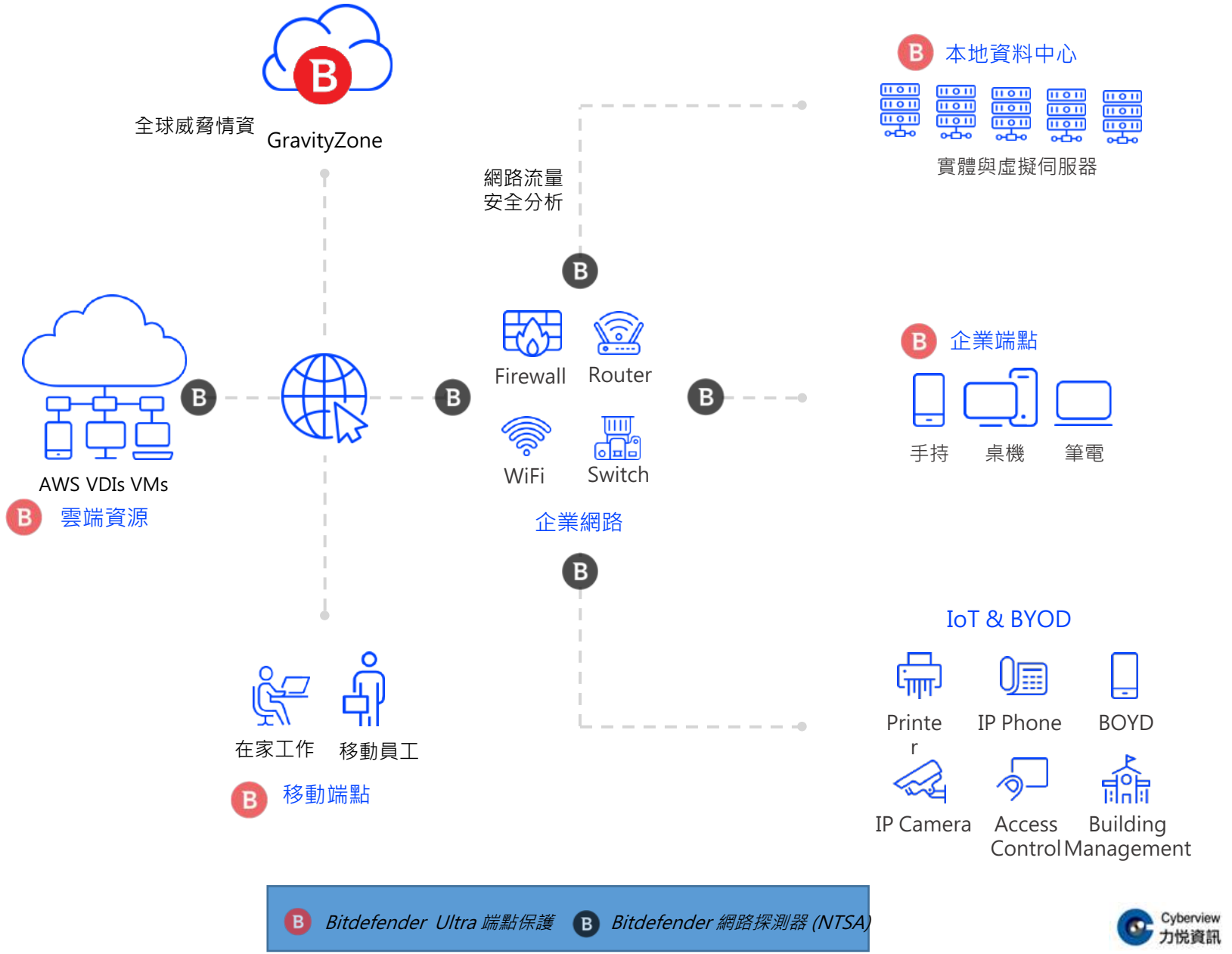
BITDEFENDER GRAVITYZONE®

@網路

Cyberview 力悦資訊

Bitdefender ULTRA & NTSA 整合式平台效益

參考架構

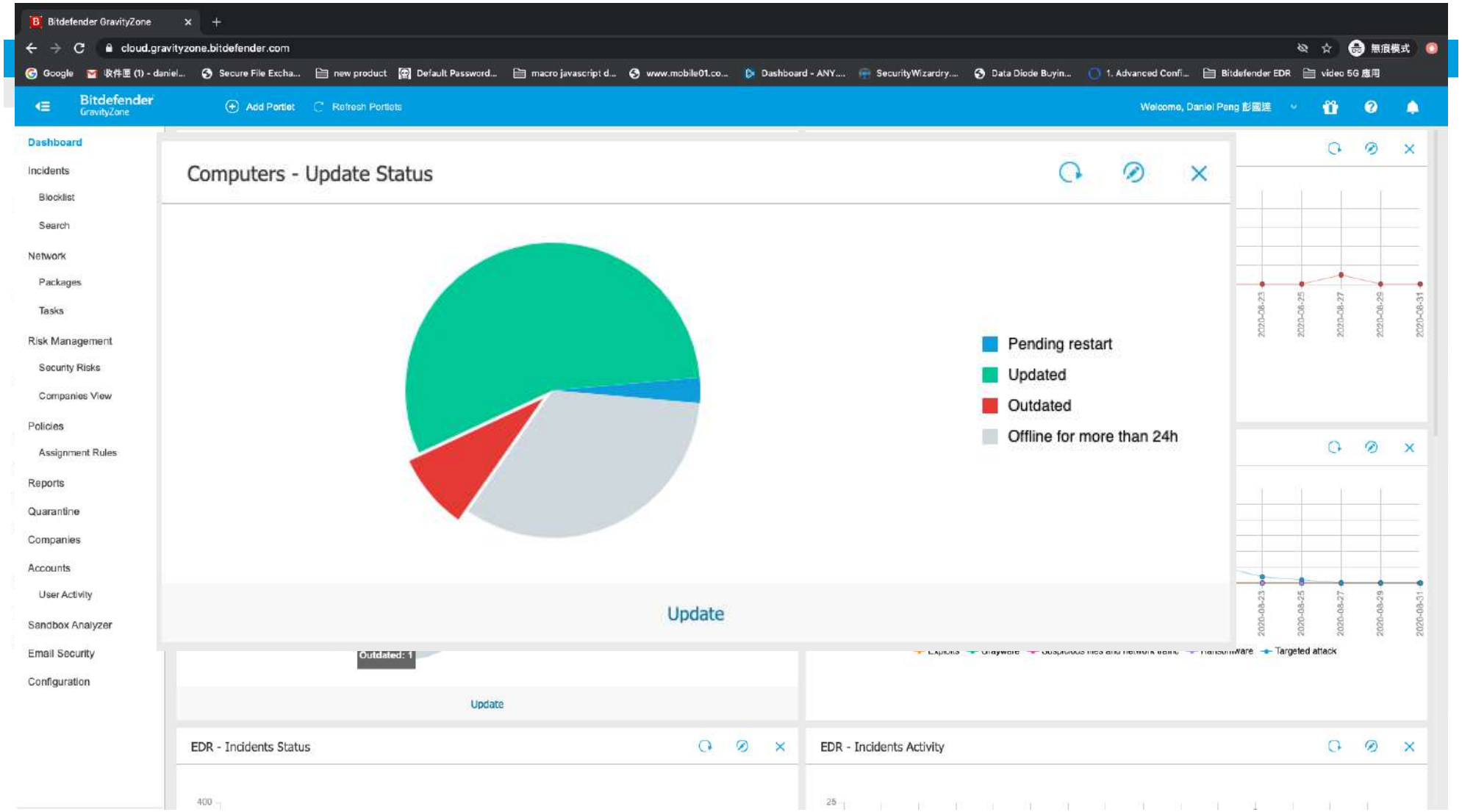


BITDEFENDER GRAVITYZONE®

@重要功能展示

中控儀表

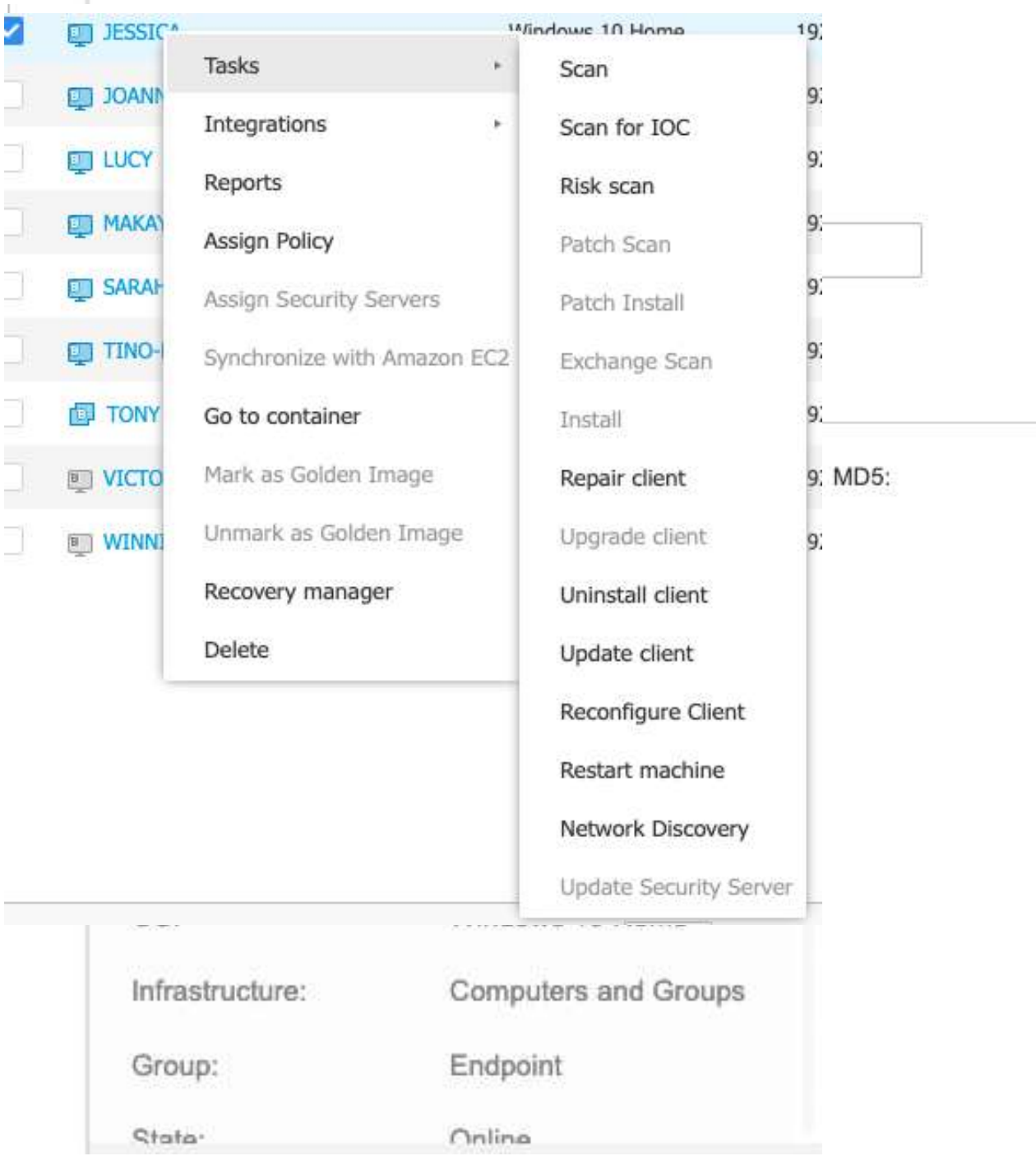
可行定義警示內容
完整drill down
自動產生報表



Cyberview 力悅資訊

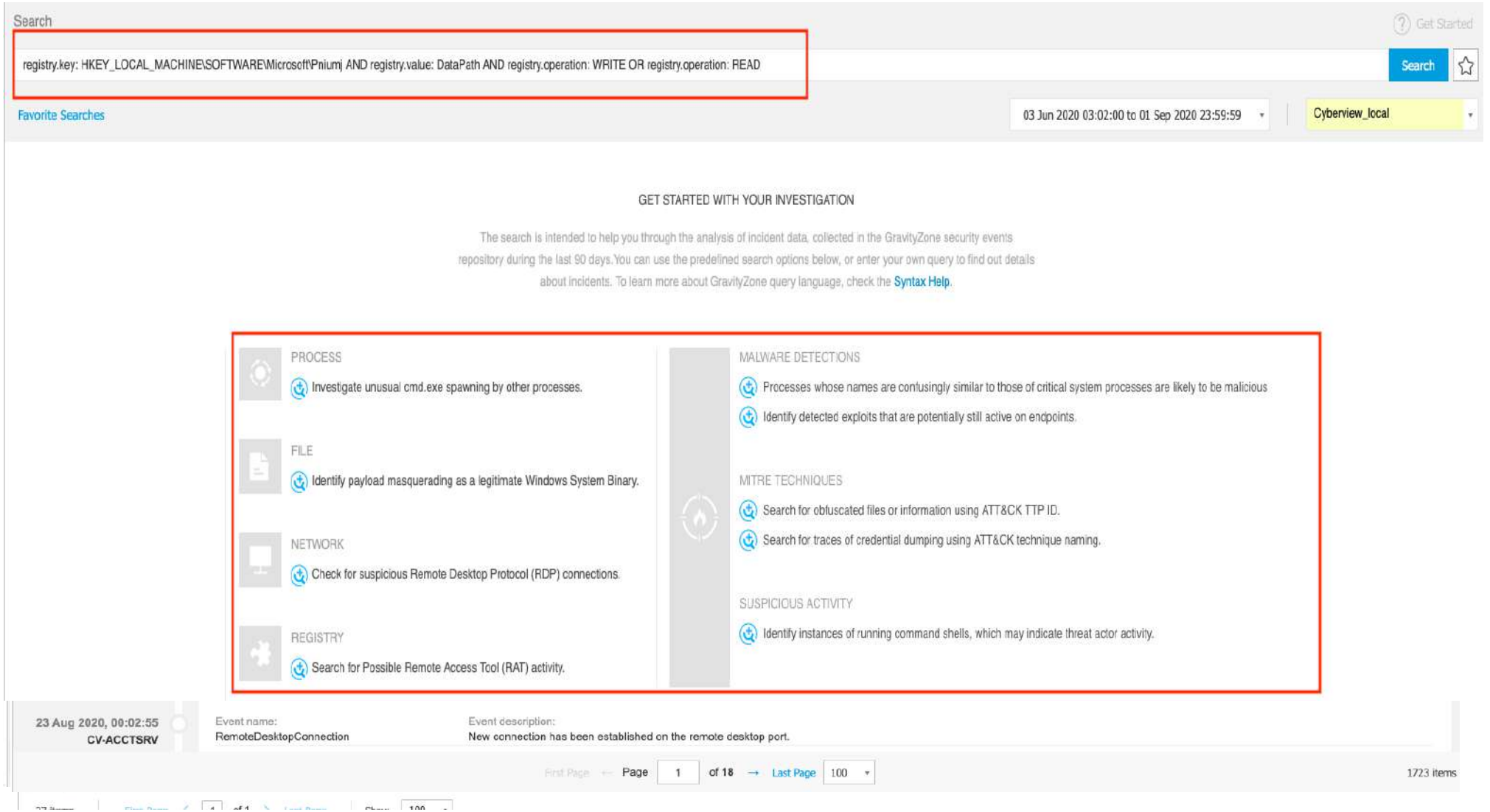
完整遠端管理

隔離&控制
Scan for IOC
一般管理



EDR

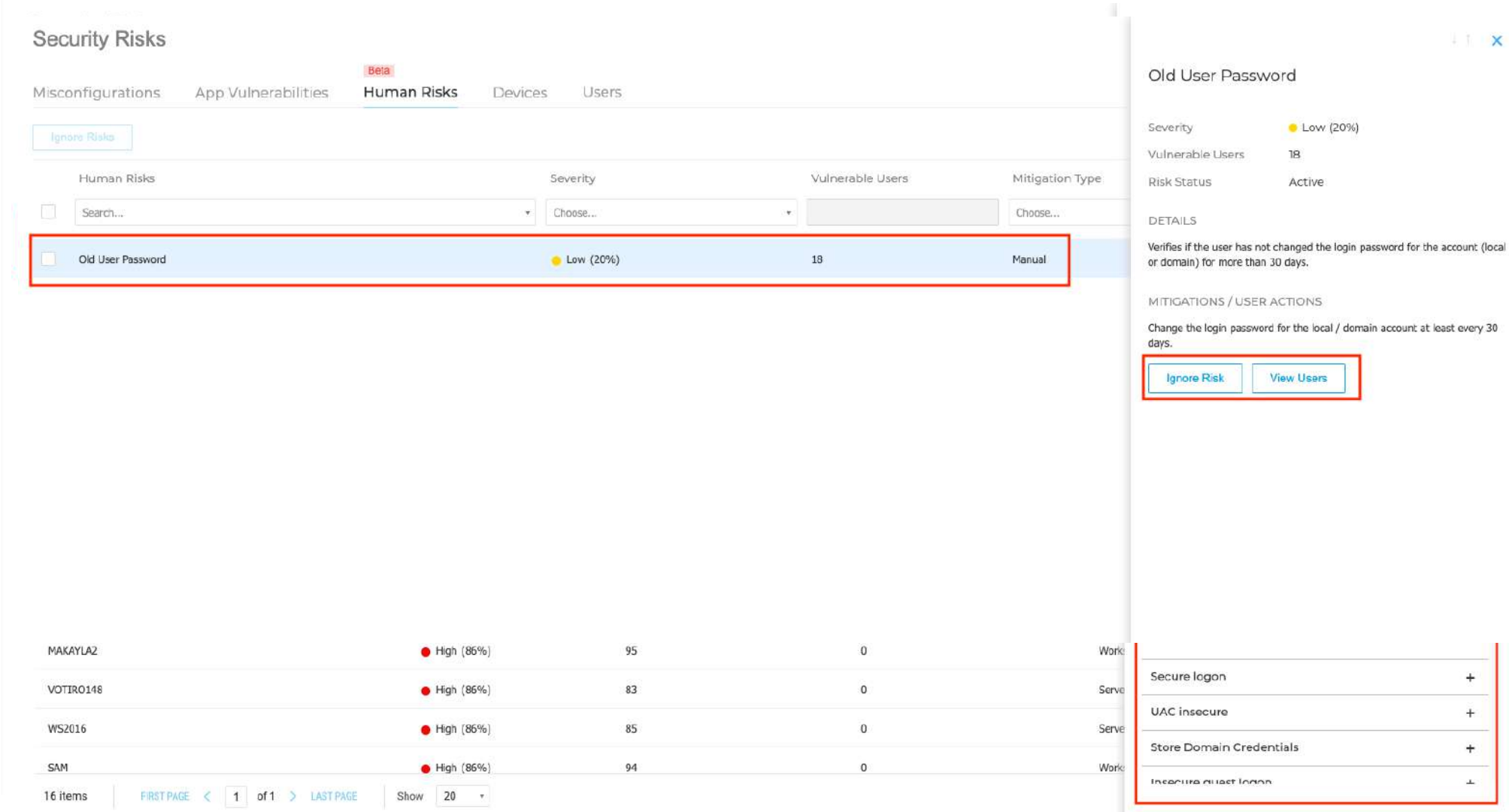
事件查詢
視覺化根因分析
時間序紀錄
完整原始資料
原始資料語法查詢



Cyberview 力悅資訊

風險分析

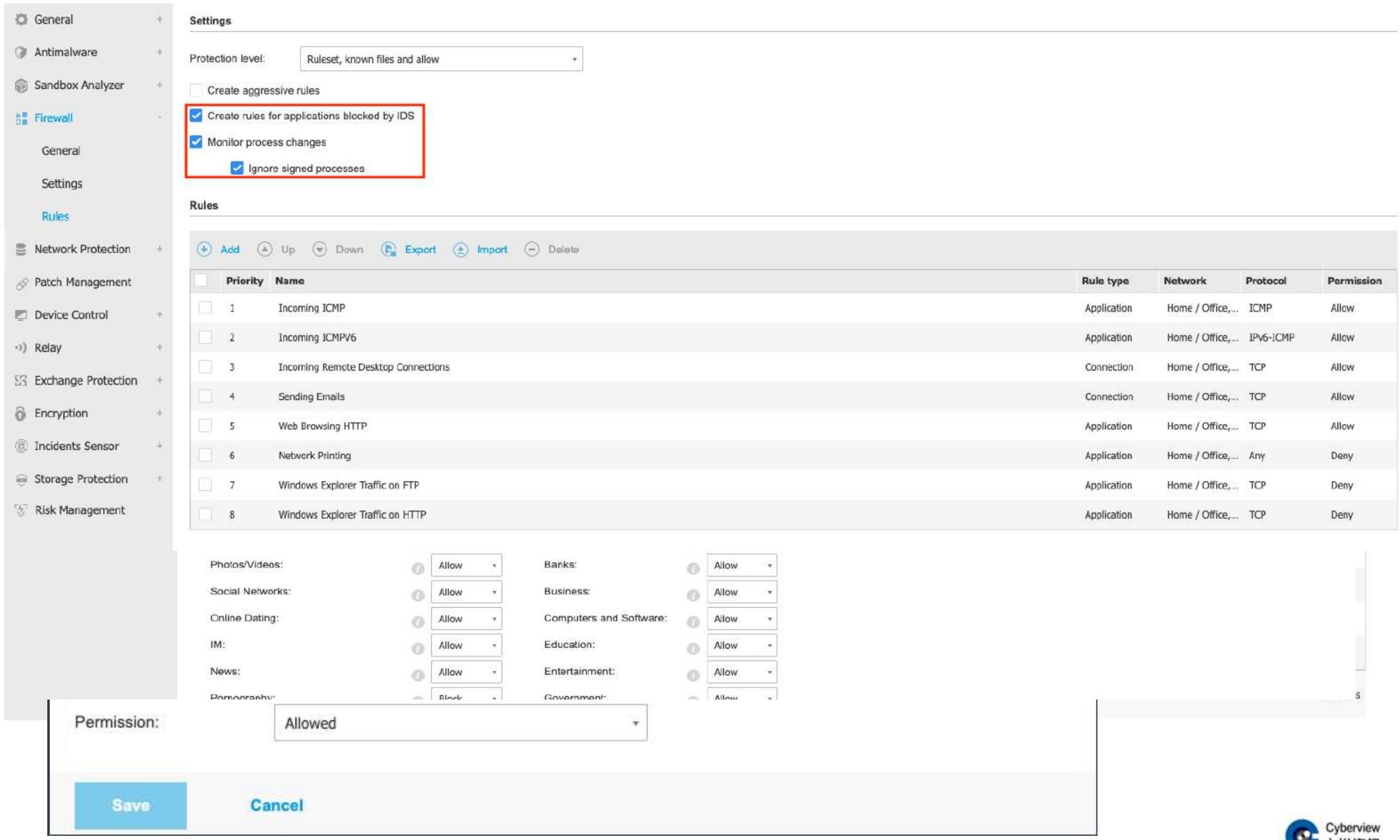
風控儀表
組態錯誤
應用程式弱點
設備總合風險
人為風險



Cyberview 力悅資訊

其它重要功能

設備控管
網站過濾
防火牆&IDS



Cyberview 力悦資訊

GRAVITYZONE APPLIANCE

GravityZone 中控站是免繁複安裝的 virtual appliance ，並且提供各種虛擬平台格式的映像檔.

➔ 運行預先強化過的 Linux 版本 (Ubuntu 16.04)

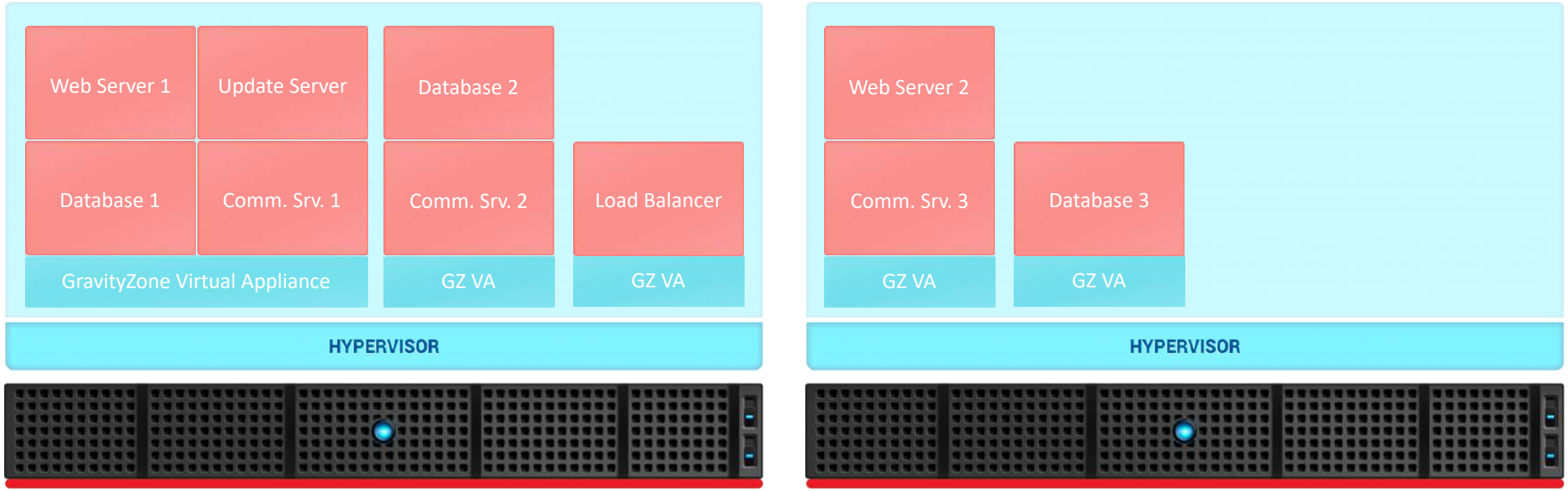
The GravityZone appliance 可以運行 一個, 多個 或 全部 以下的角色:

- Database(資料庫)
- Update Server(特徵碼更新服務)
- Web Server (Web Console 管理介面)
- Communication Server (端點聯繫溝通服務)

GravityZone 部署時要求至少包含一個角色.

根據架構的大小與 GravityZone 的分佈, 您可以運行一個到多個 GravityZone appliances.

跨主機的多中心含分散式資料庫部署

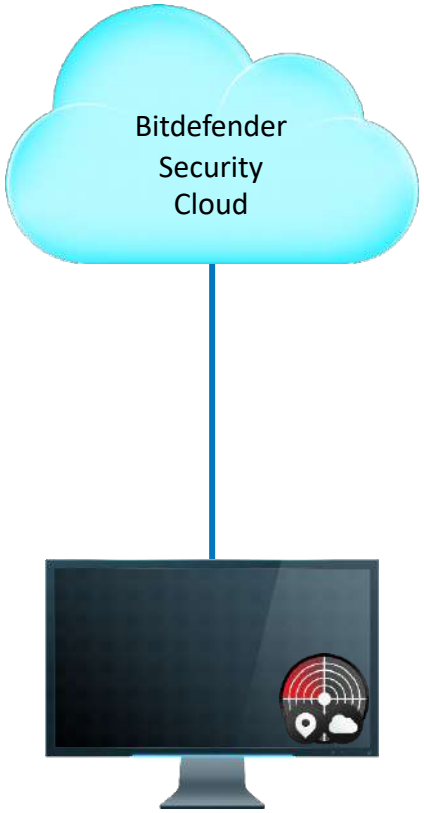


Bitdefender

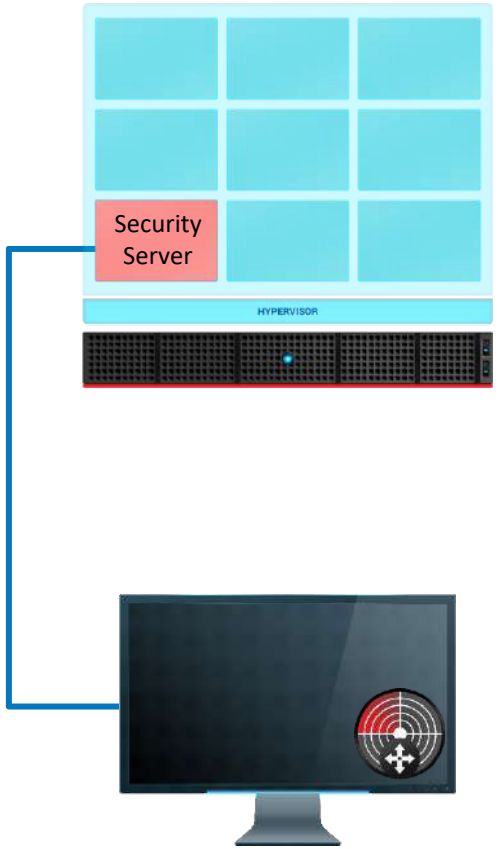
Cyberview 力悅資訊

端點的安全防護
最棒的掃描引擎

本地(Local) Scan



混合(Hybrid) Scan

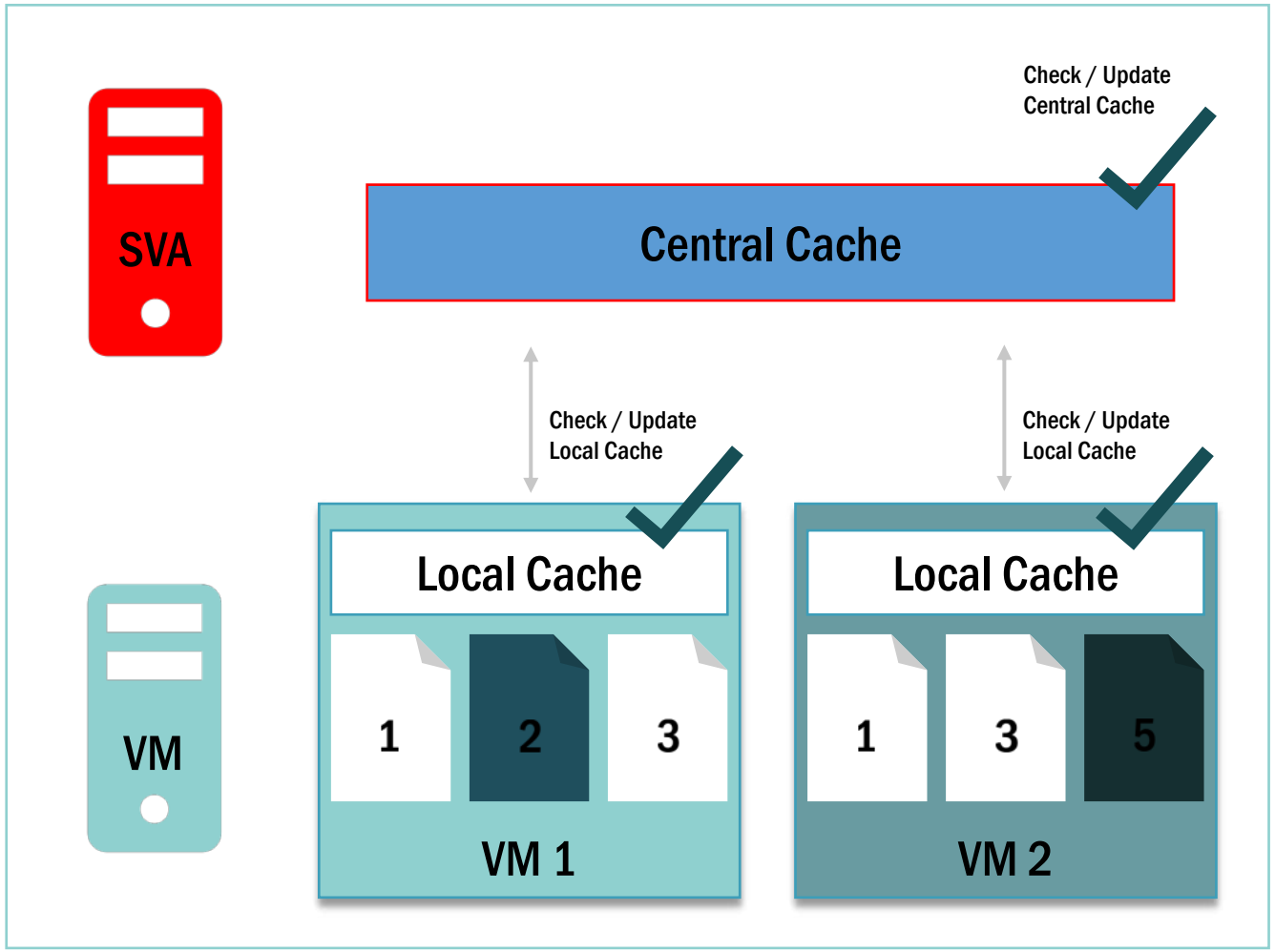


中央(Central) Scan

Bitdefender

Cyberview 力悦資訊

SECURITY SERVER
PATENTED TWO-LEVEL CACHING



Two-level caching有效提高 VM(virtual machine) 和 SVA(security virtual appliance) 的反惡意軟件效率

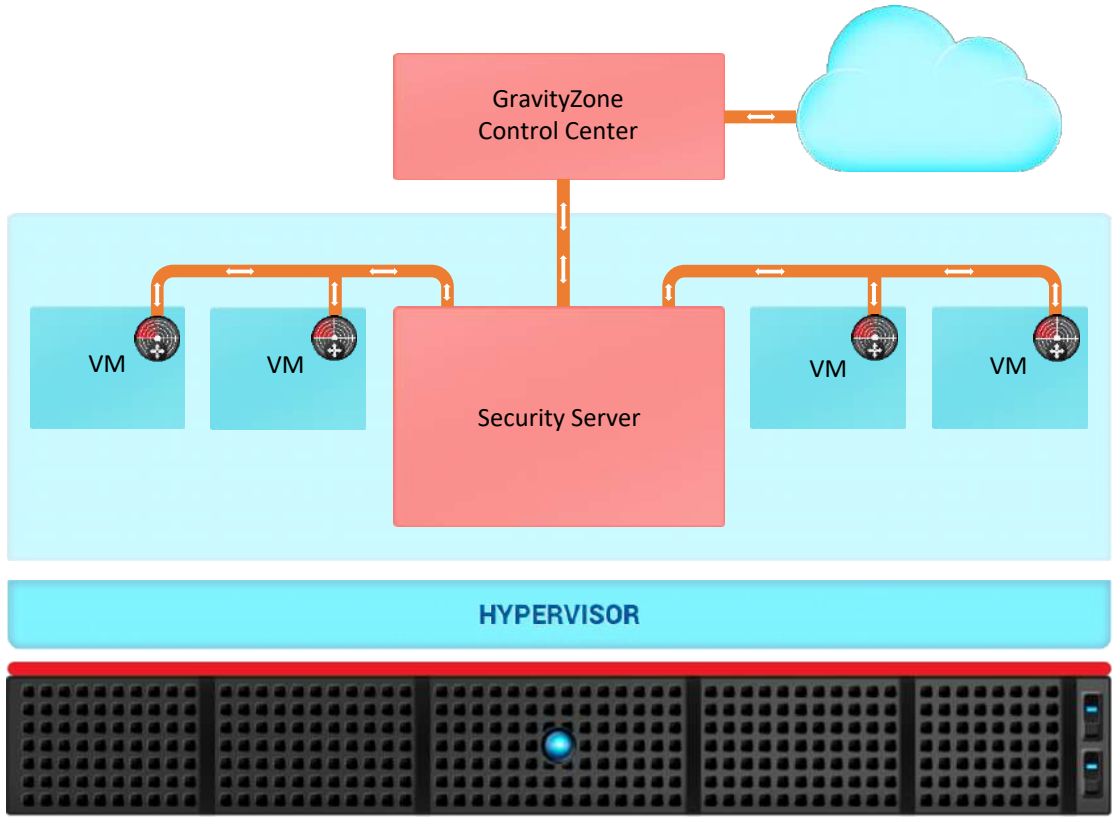
SVA僅檢查每個文件一次，即使它出現在多個VMs上也是如此

這有助於避免冗餘掃描，從而顯著減少CPU，RAM，I/O和網絡負載

Bitdefender

Cyberview 力悦資訊

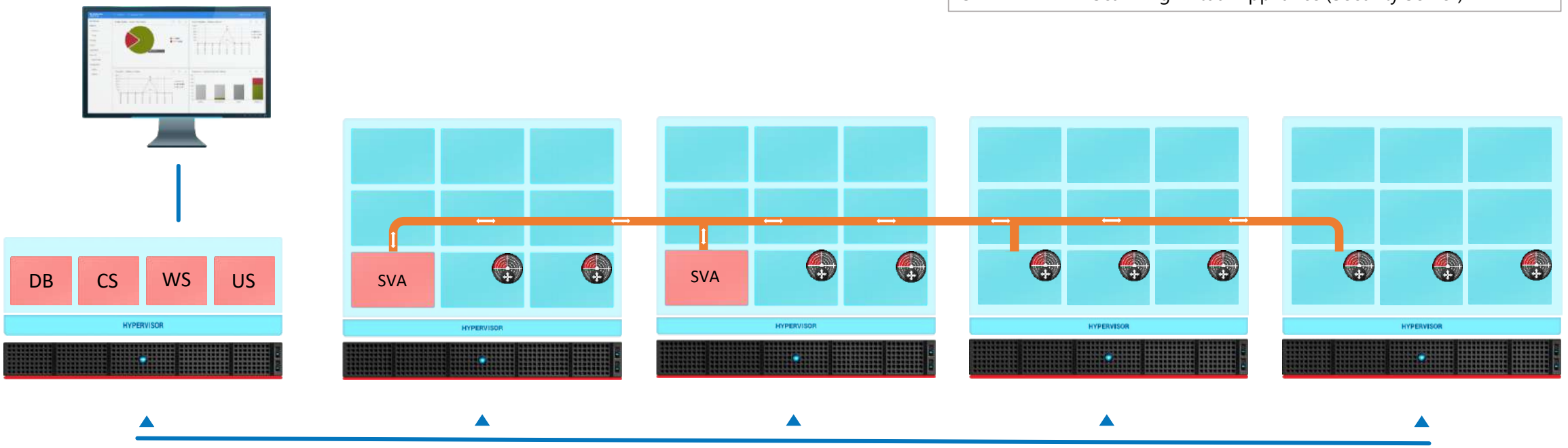
SECURITY FOR VIRTUALIZED ENVIRONMENTS
MULTIPLATFORM ARCHITECTURE (VMWARE)



BEST with Central Scan

SECURITY FOR VIRTUALIZED ENVIRONMENTS
MULTIPLATFORM ARCHITECTURE (NUTANIX, CITRIX)

DB	Database
CS	Communication Server
WS	Web Server
US	Update Server
SVA	Scanning Virtual Appliance (Security Server)

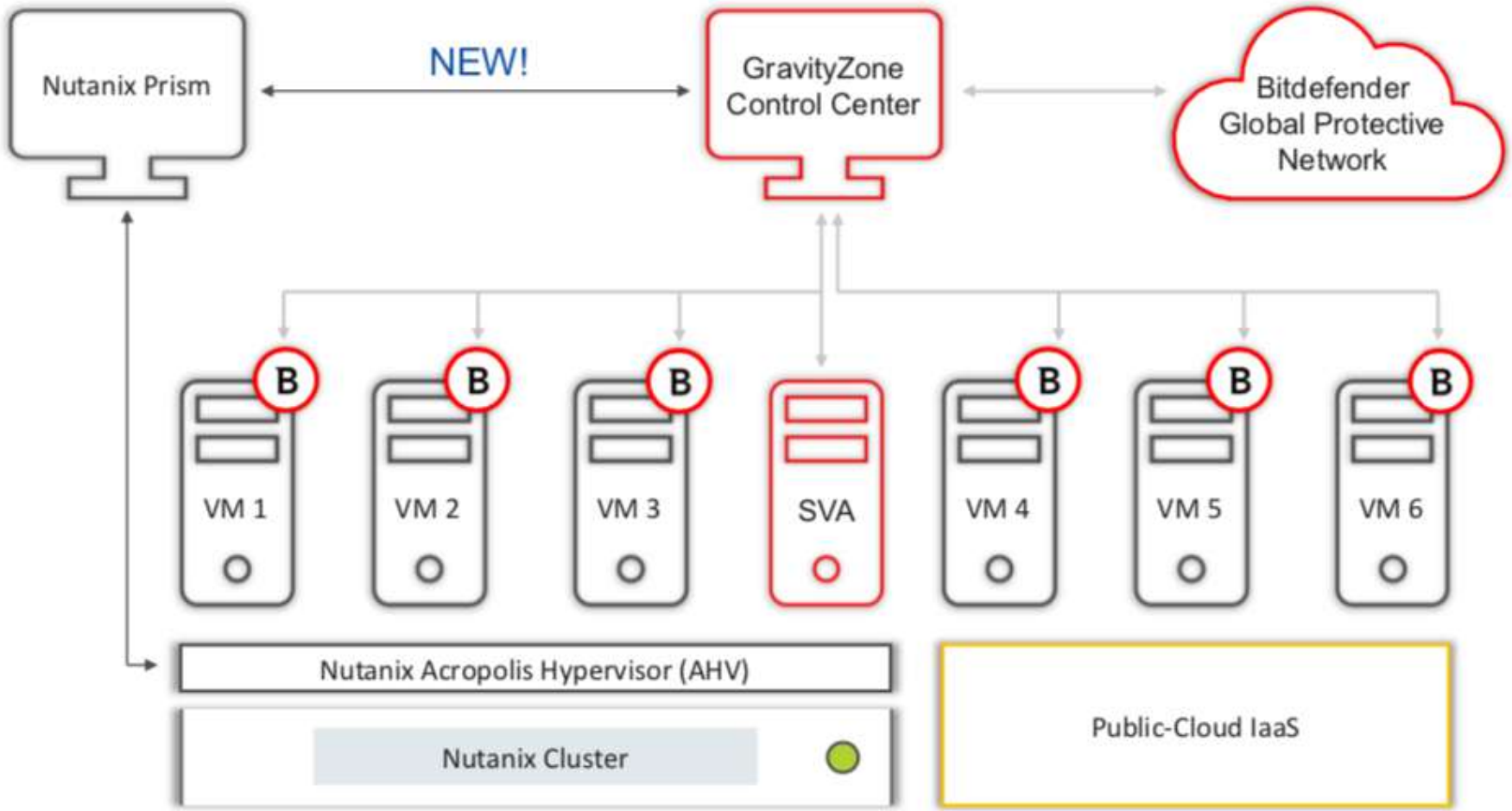


Bitdefender

Cyberview 力悦資訊

SECURITY FOR VIRTUALIZED ENVIRONMENTS

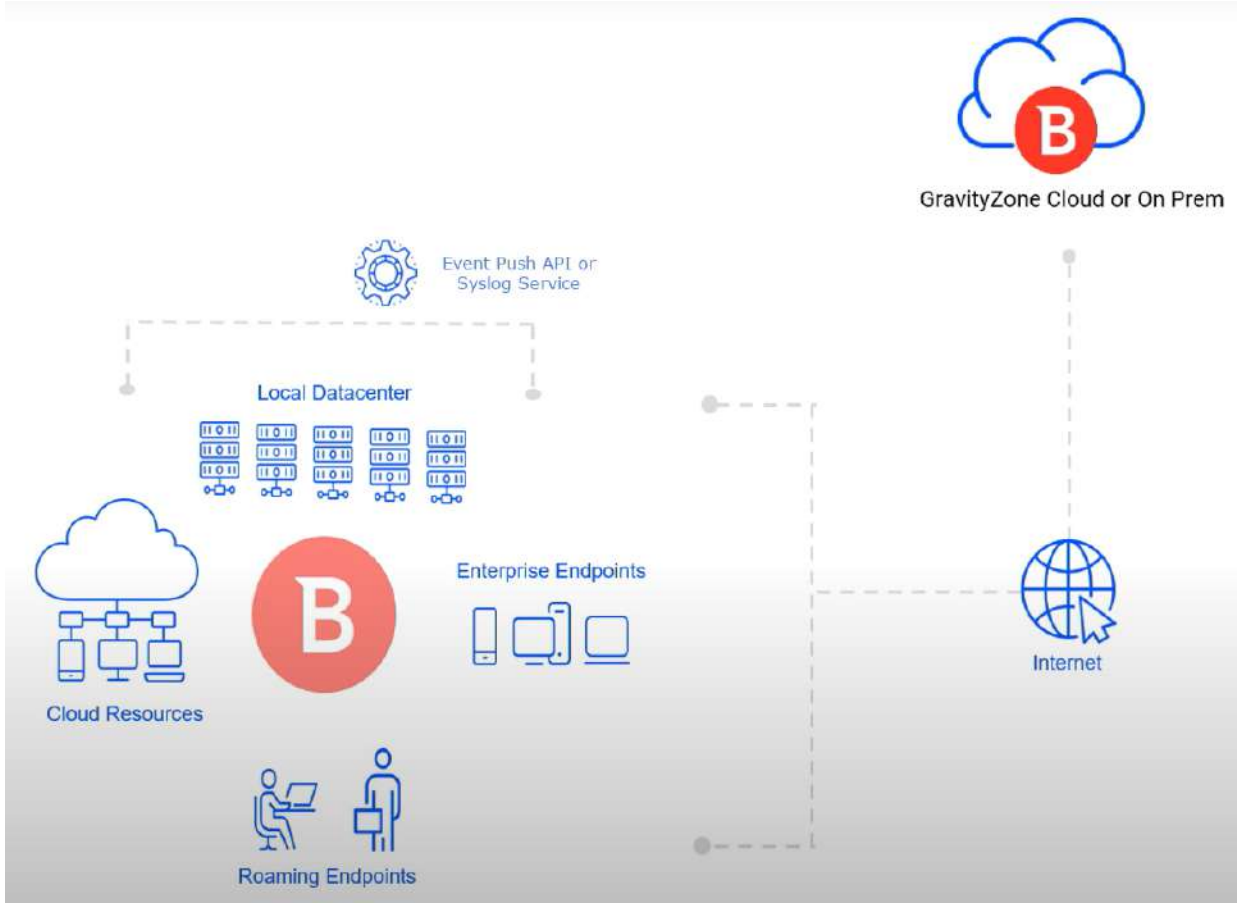
整合虛擬機管理介面，AGENT自動佈建、回收

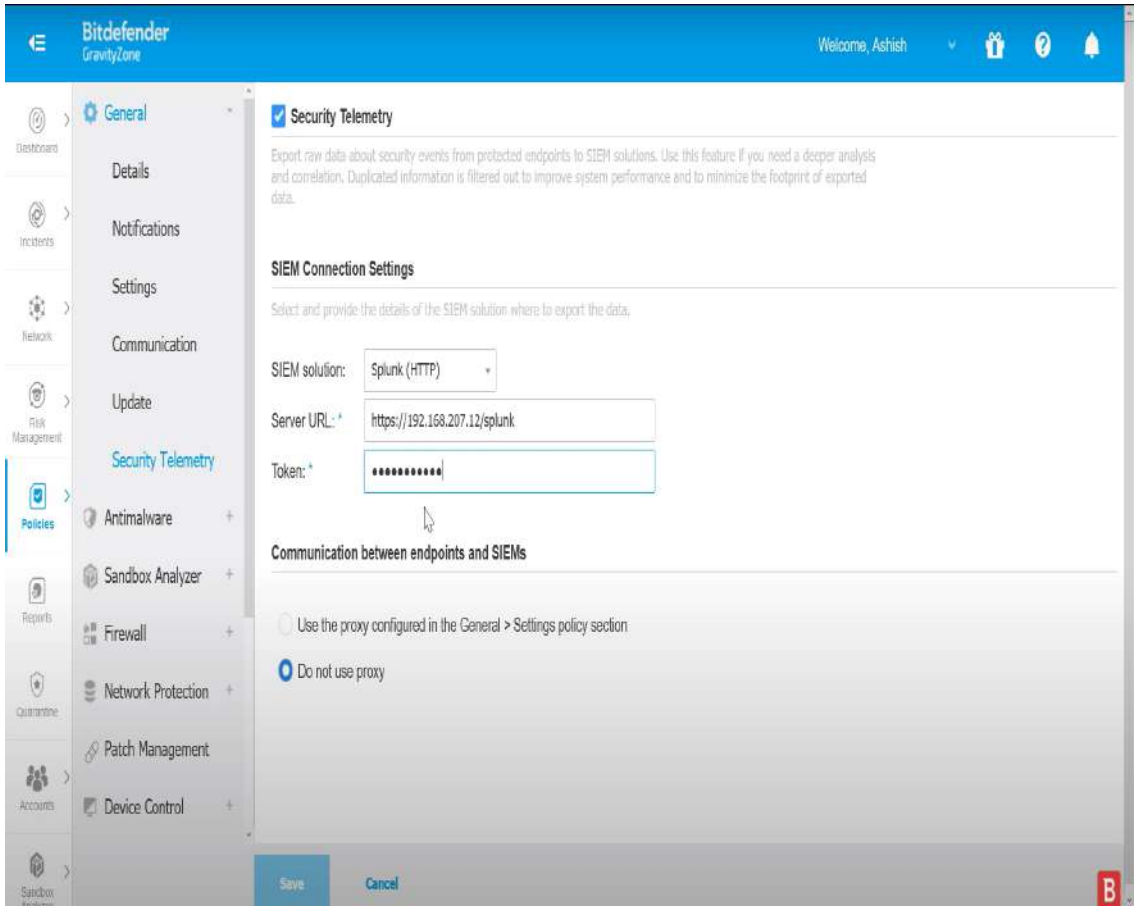


BEST with Central Scan

Cyberview 力悦資訊

事件與RAW DATA轉發至SIEM

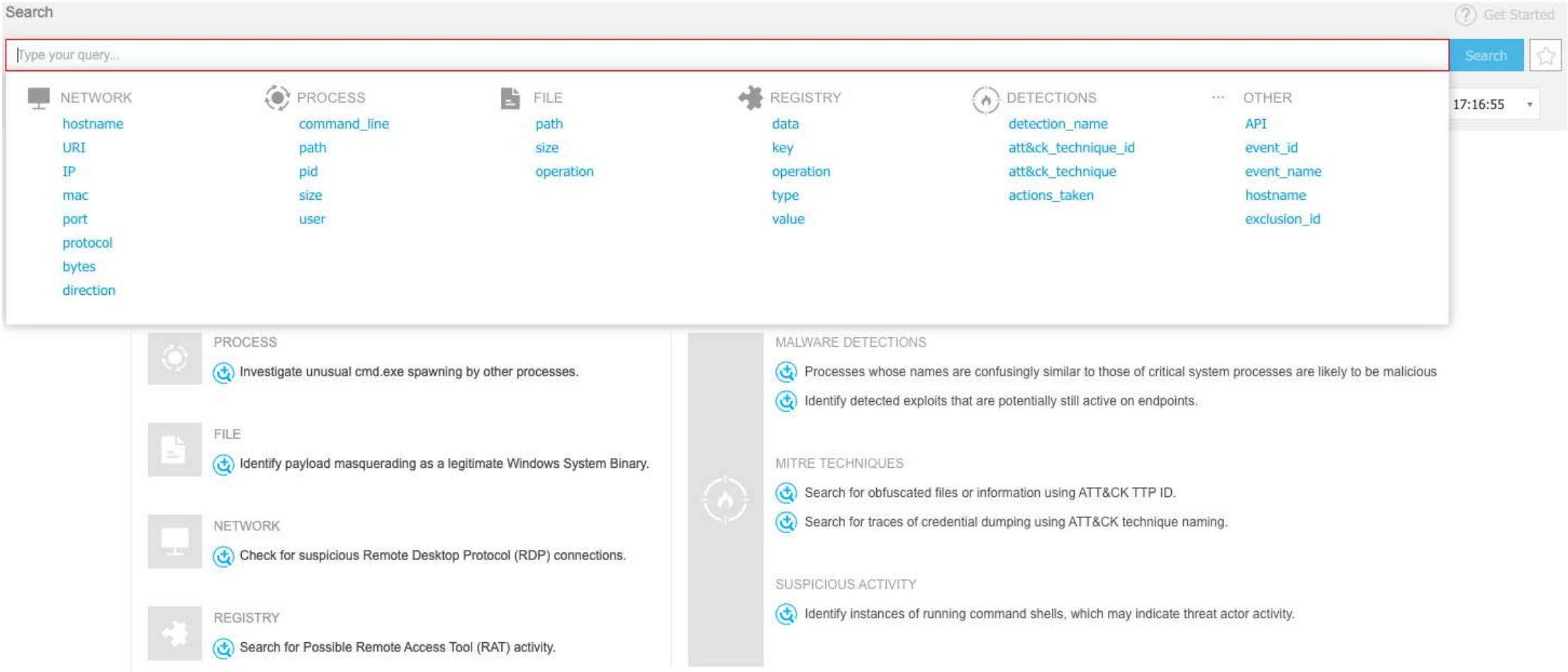




Bitdefender

Cyberview 力悦資訊

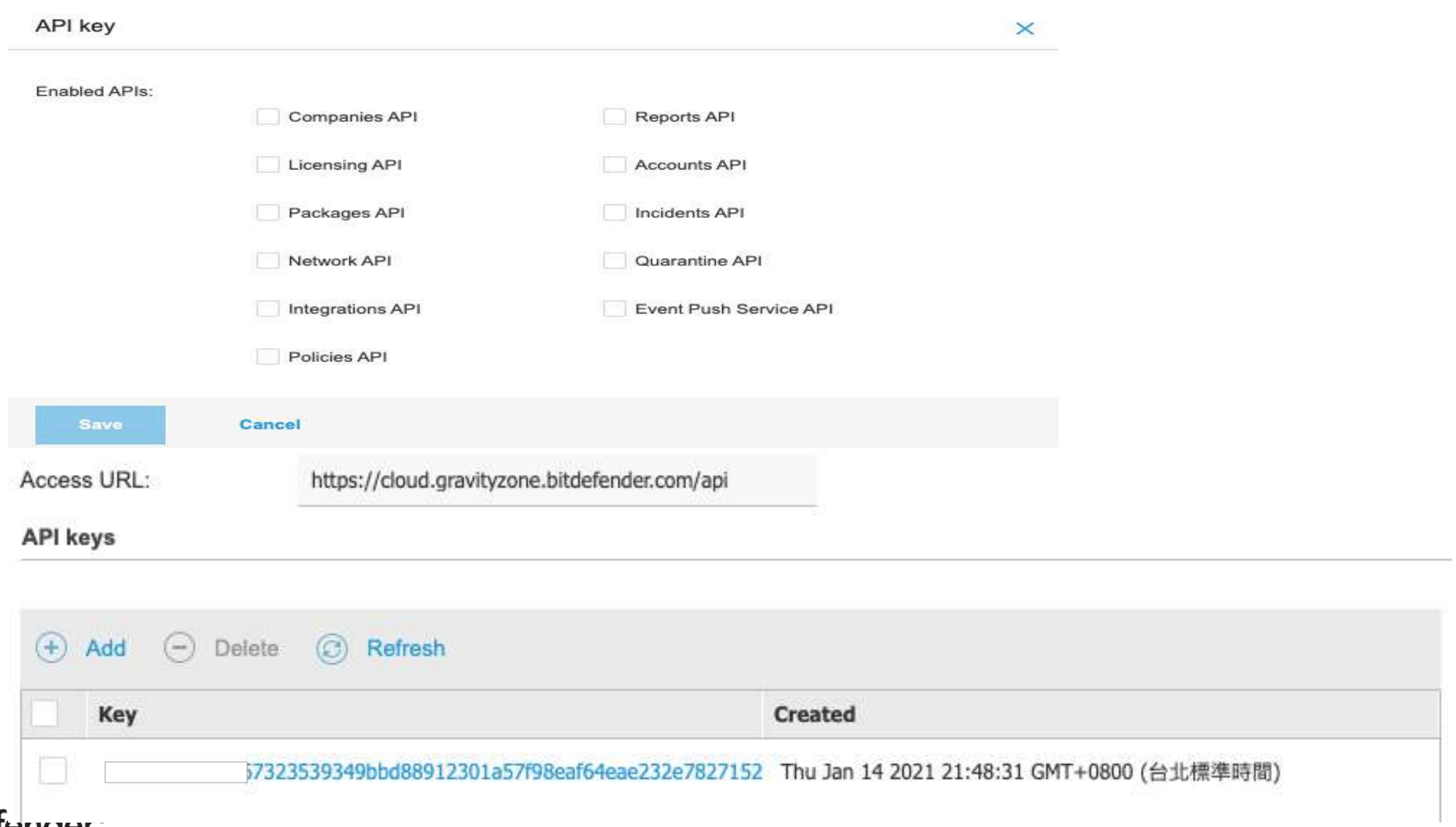
RAW DATA支援搜尋(CLOUD版)地端使用SIEM



Bitdefender

Cyberview 力悅資訊

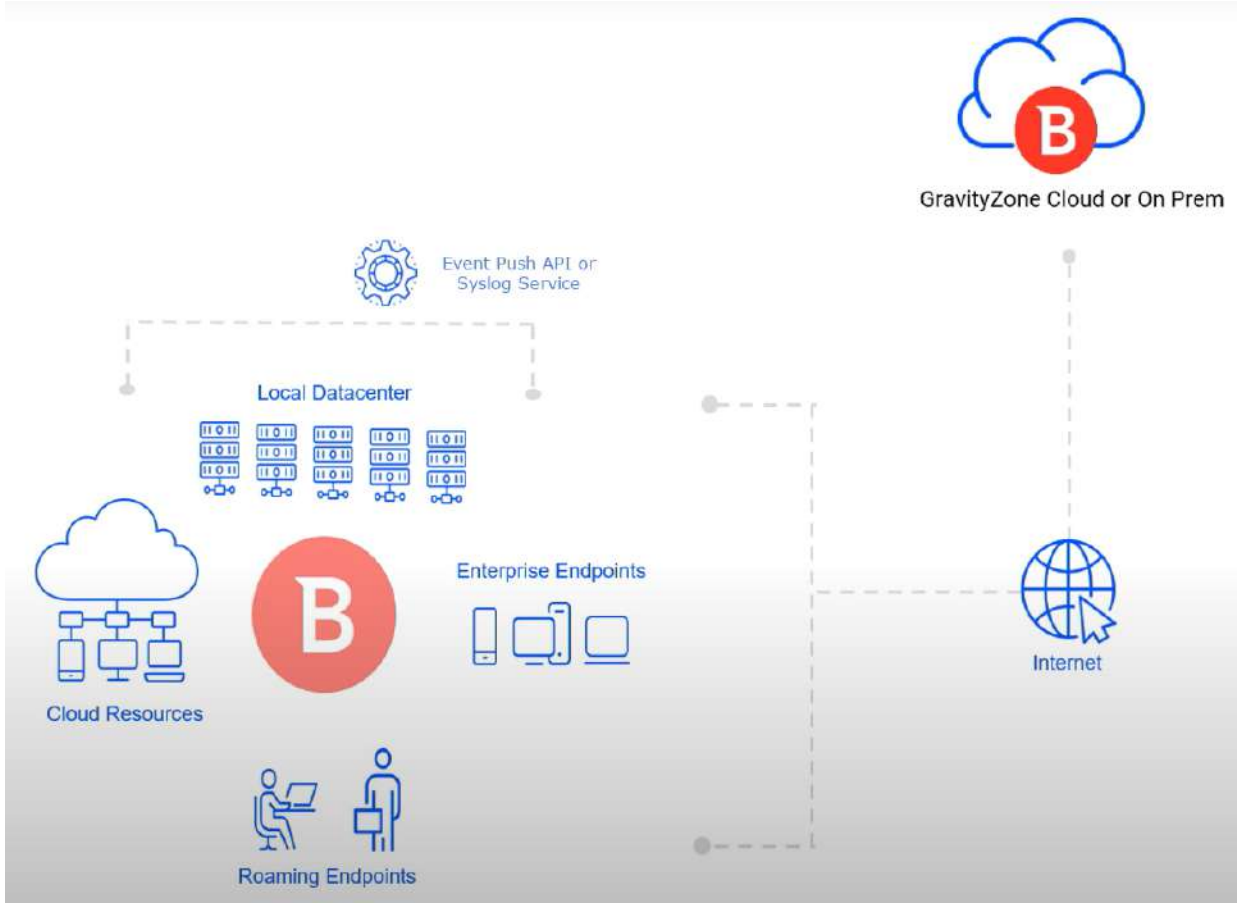
整合性(一)：全功能API

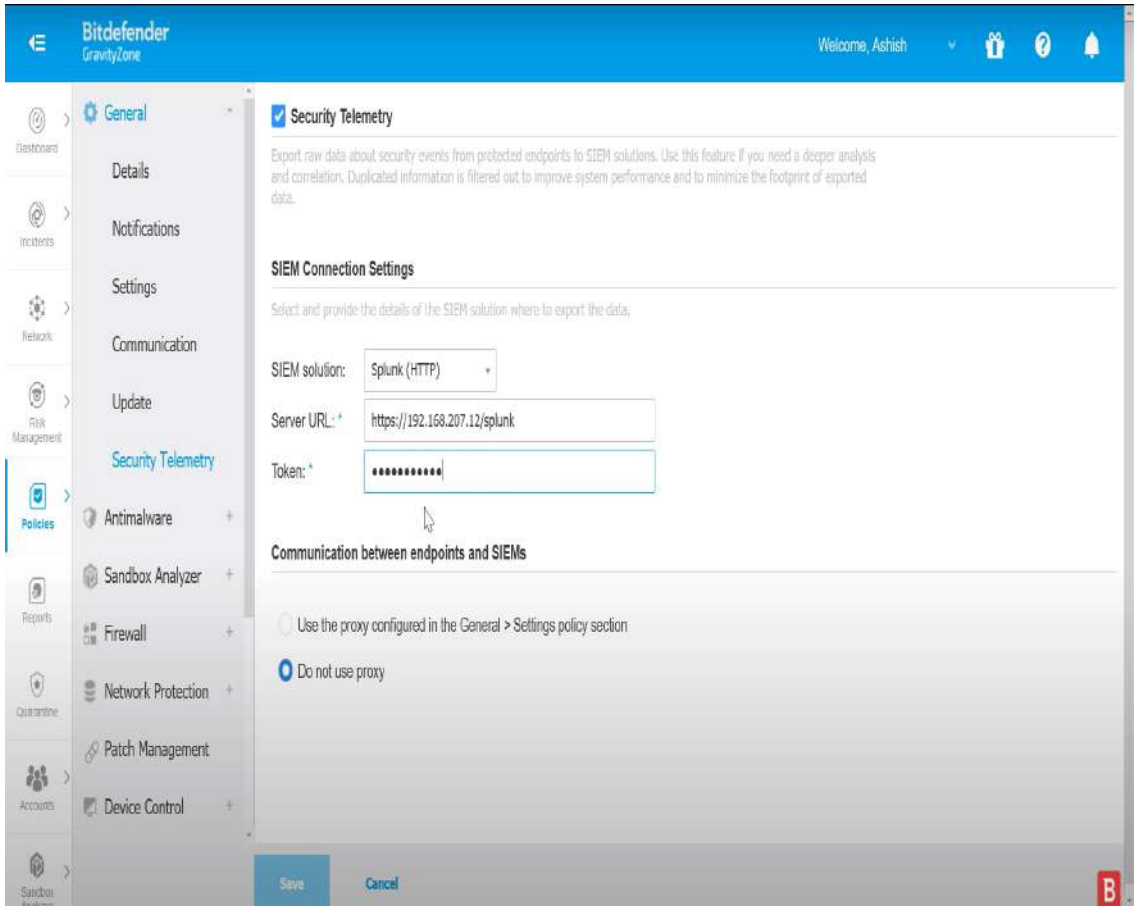


Bitdefender

Cyberview 力悦資訊

整合性(二)：SIEM

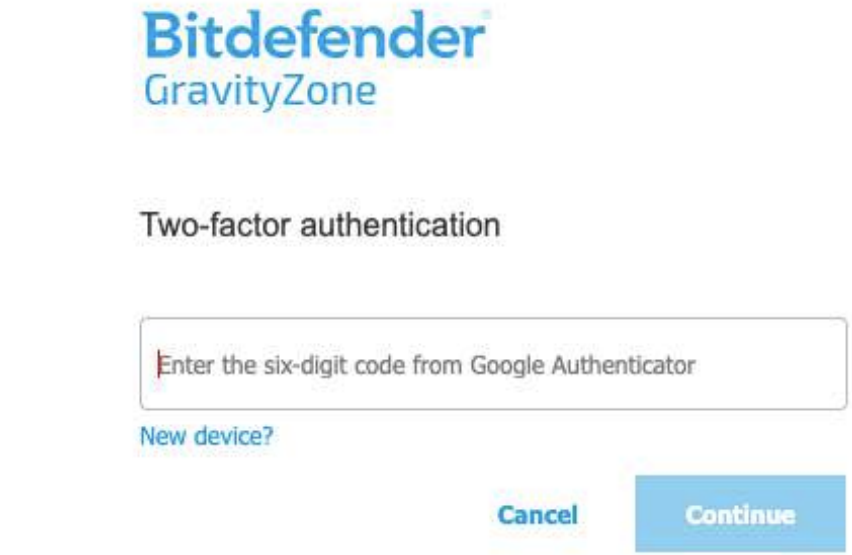




Bitdefender

Cyberview 力悦資訊

整合性(三)：2FA (RFC6238) & AD (電腦, 帳號) & SSO(SAML)



Bitdefender

Cyberview 力悦資訊

Q&A

Cyberview 力悦資訊

THANK YOU!

Cyberview 力悦資訊

超越EDR-唯有Bitdefender &
精誠資安實戰
相見恨晚

精誠資訊股份有限公司
企業創新應用事業部
售前顧問:林宗翰HANK
HANKLIN@SYSTEX.COM

駭客網路攻擊練七階段

您對縱深防禦安全的解讀是?

邊界防火牆

DDoS

應用程式防火牆(WAF)

EDR

防毒

入侵偵測(IDS)/防禦(IPS)

UEBA(使用者/設備行為分析)

SIEM

你的資訊環境安全嗎?

即便是超級跑車，行為不正確實還是有機會撞毀

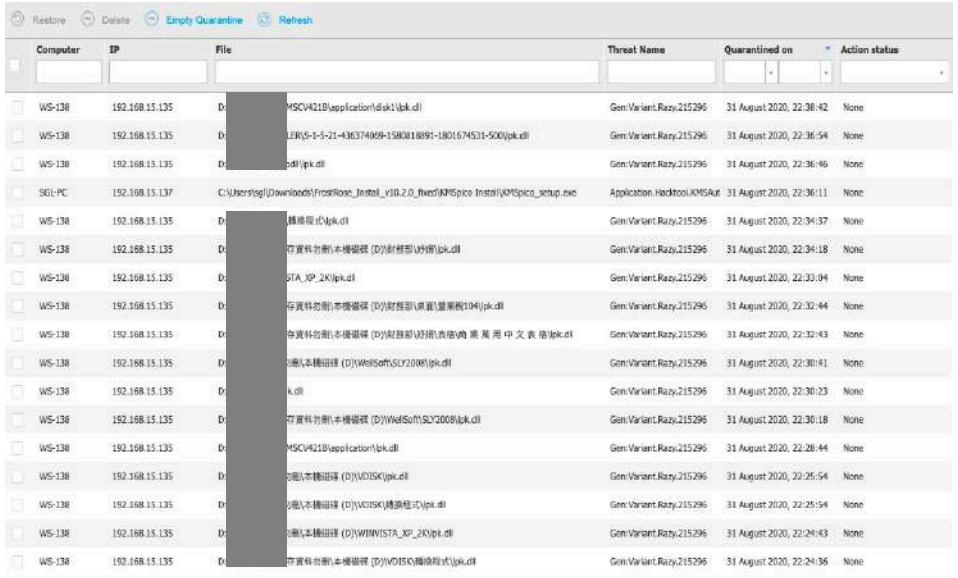
實戰案例一

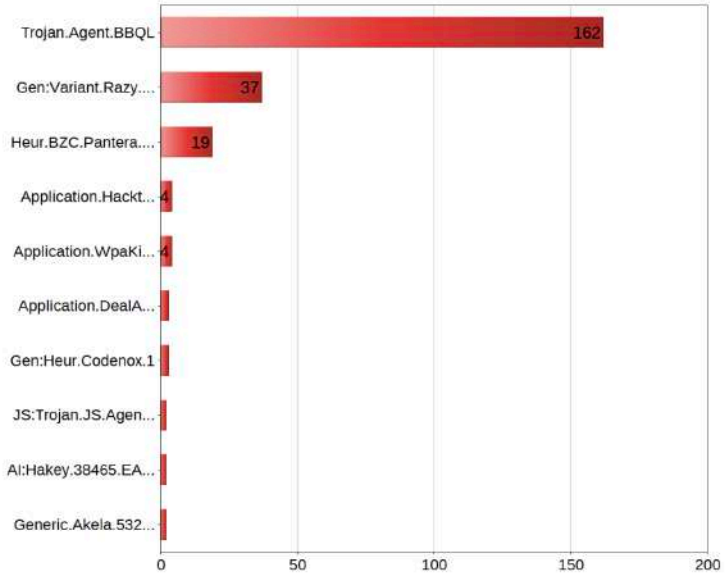
駭客

駭客入侵

企業

資料外洩使得
詐騙集團勒索民眾



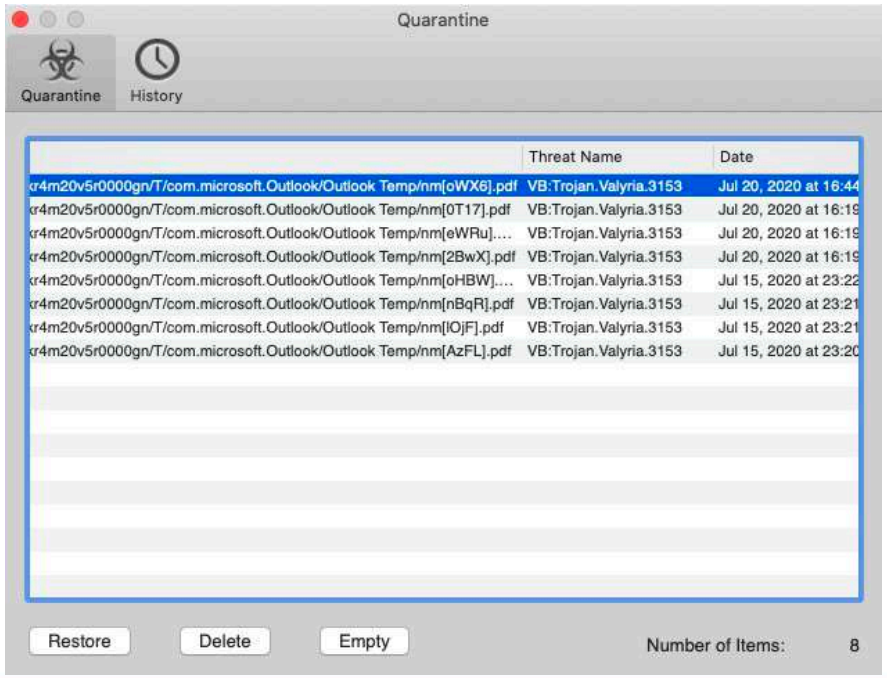


實戰案例二

Xpcproxy Mac

漏洞

APT32代號：海上蓮花OceanLotus



各項模組的整合

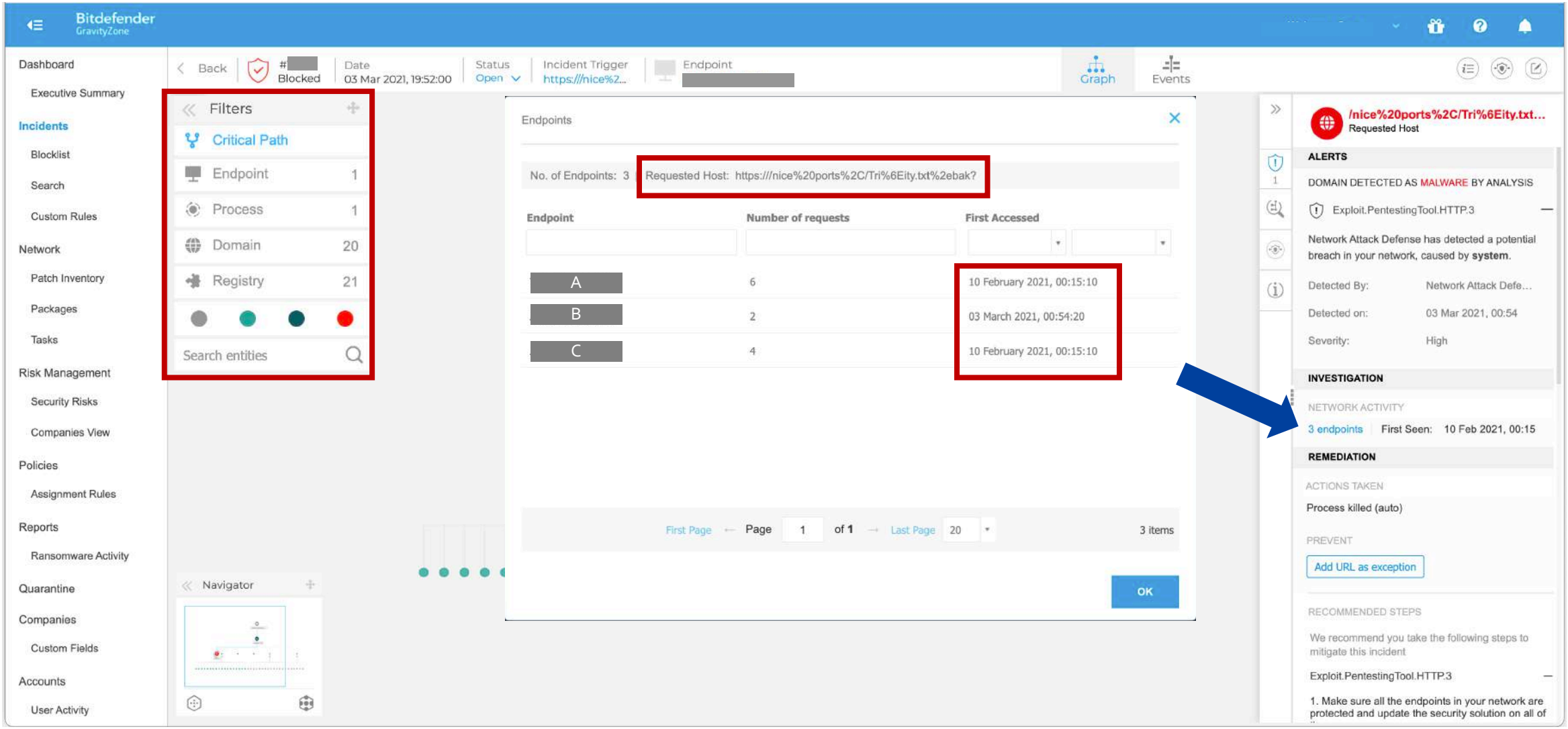
預防

強化 & 控制

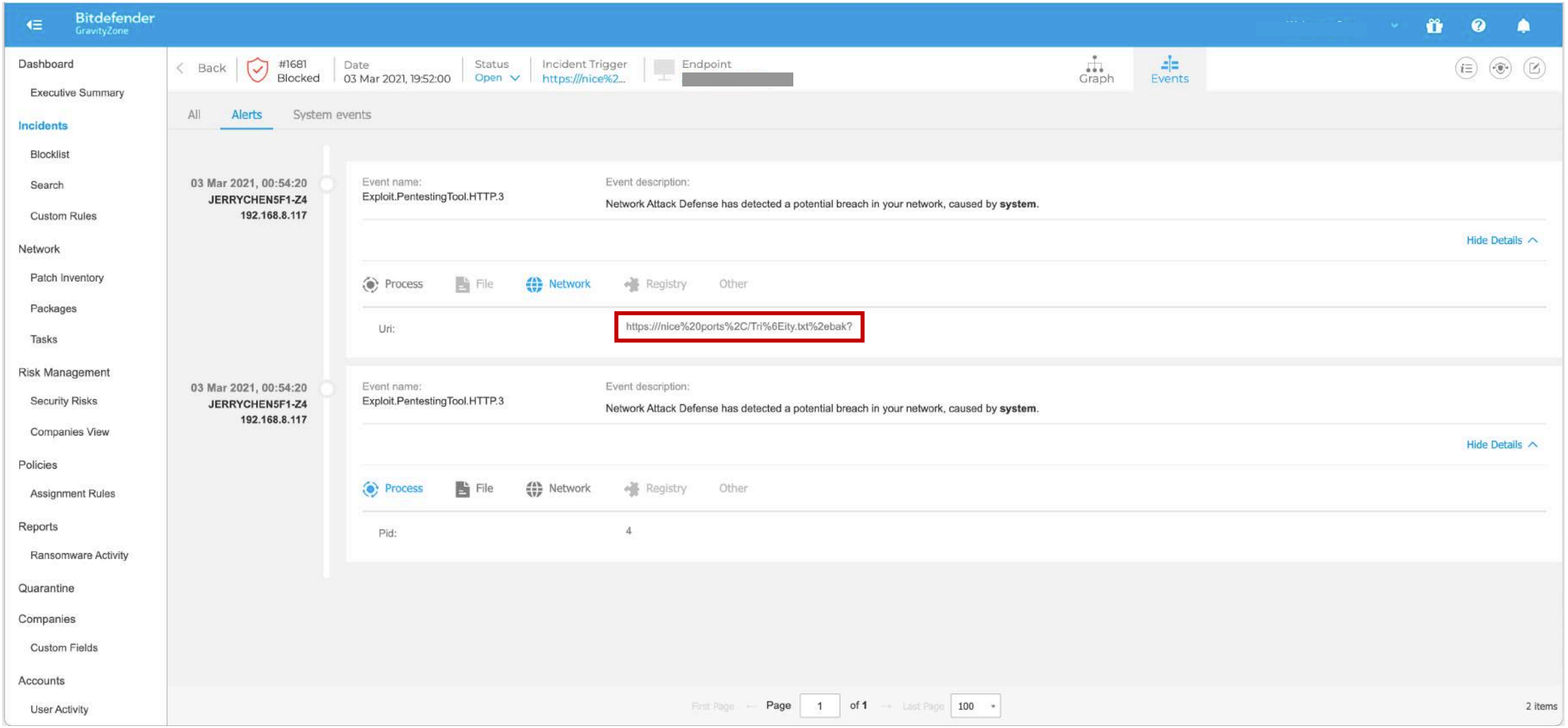
偵測 & 反應

服務

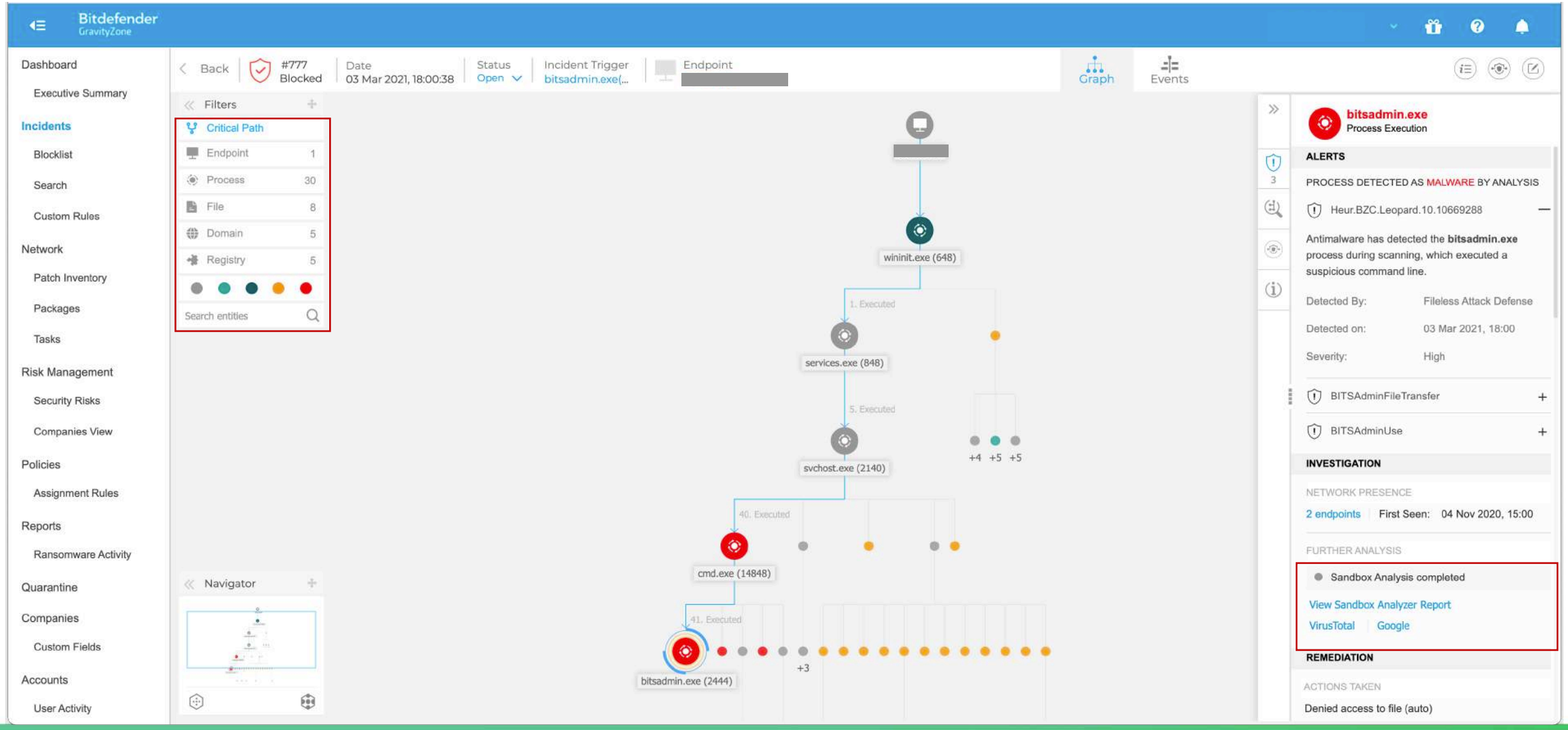
實戰案例三



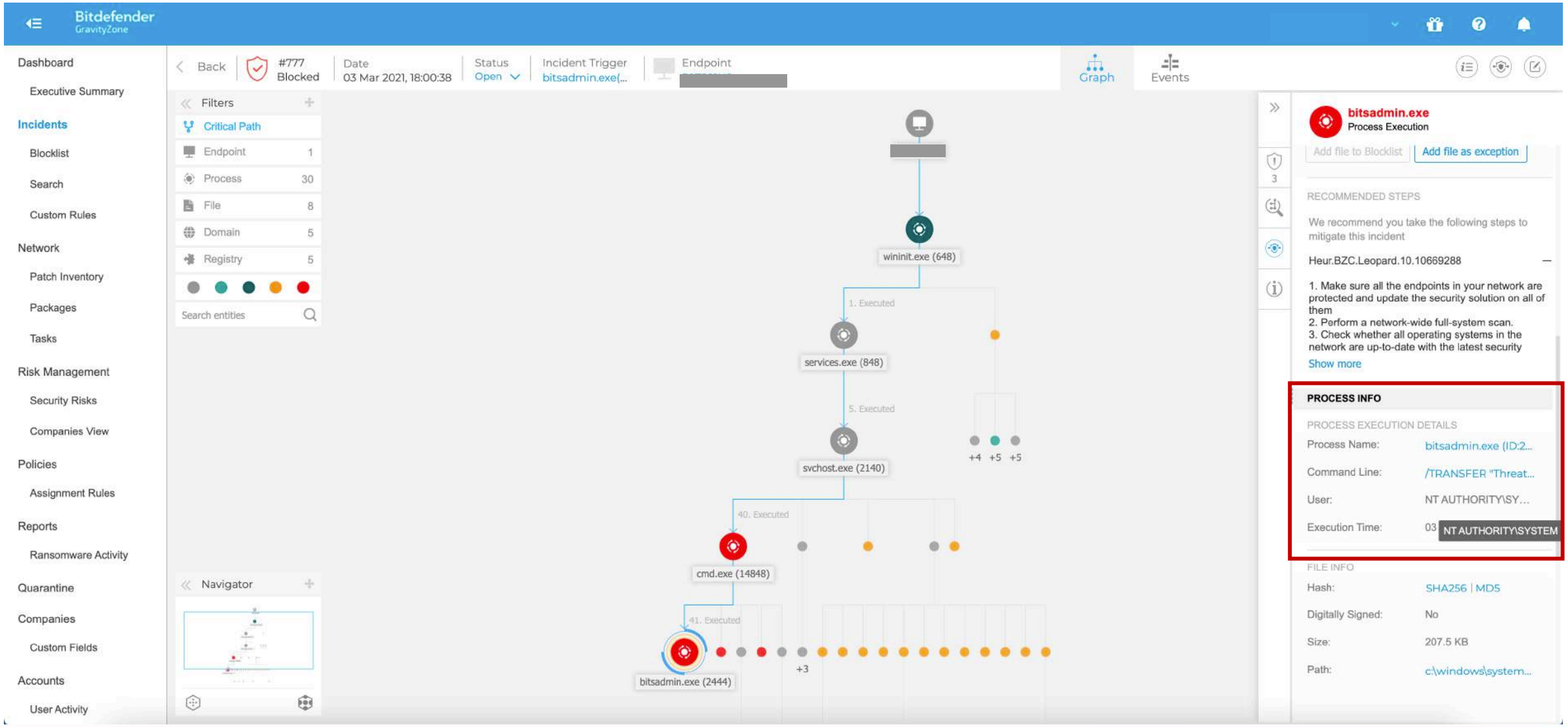
實戰案例三



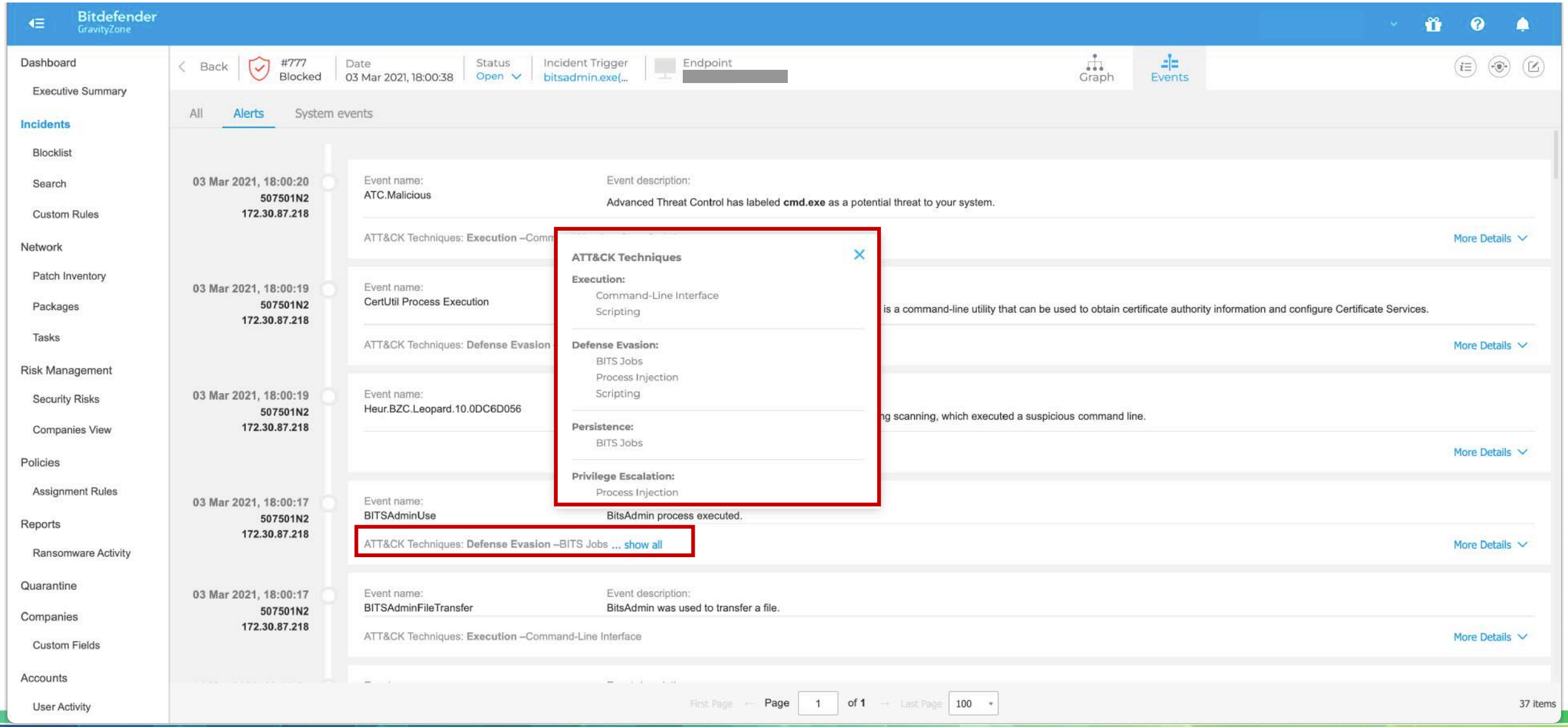
實戰案例四



實戰案例四



實戰案例四



Bitdefender與MITRE ATT&CK攻擊手法名稱一致

interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

The interface to create and manage BITS jobs is accessible through PowerShell [2] and the BITSAdmin tool. [3]

Adversaries may abuse BITS to download, execute, and even clean up after running malicious code. BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls. [4] [5] [6] BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots). [7] [4]

BITS upload functionalities can also be used to perform Exfiltration Over Alternative Protocol. [4]

Tactics: Defense Evasion, Persistence

Platforms: Windows

Permissions Required: Administrator, SYSTEM, User

Data Sources: Packet capture, Process command-line parameters, Process monitoring, Windows event logs

Defense Bypassed: Firewall, Host forensic analysis

Contributors: Red Canary; Ricardo Dias

Version: 1.1

Created: 18 April 2018

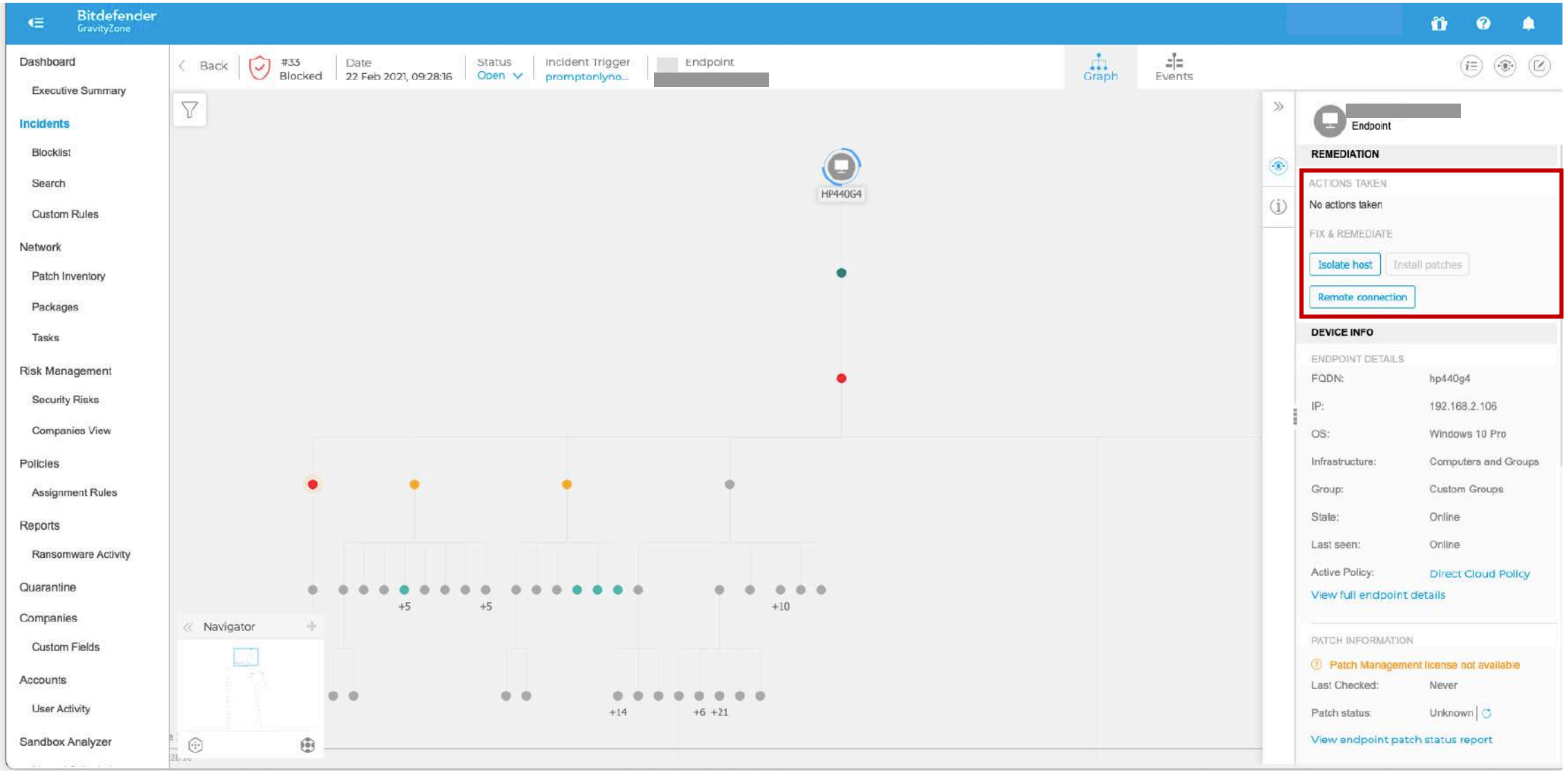
Last Modified: 25 March 2020

Version Permalink

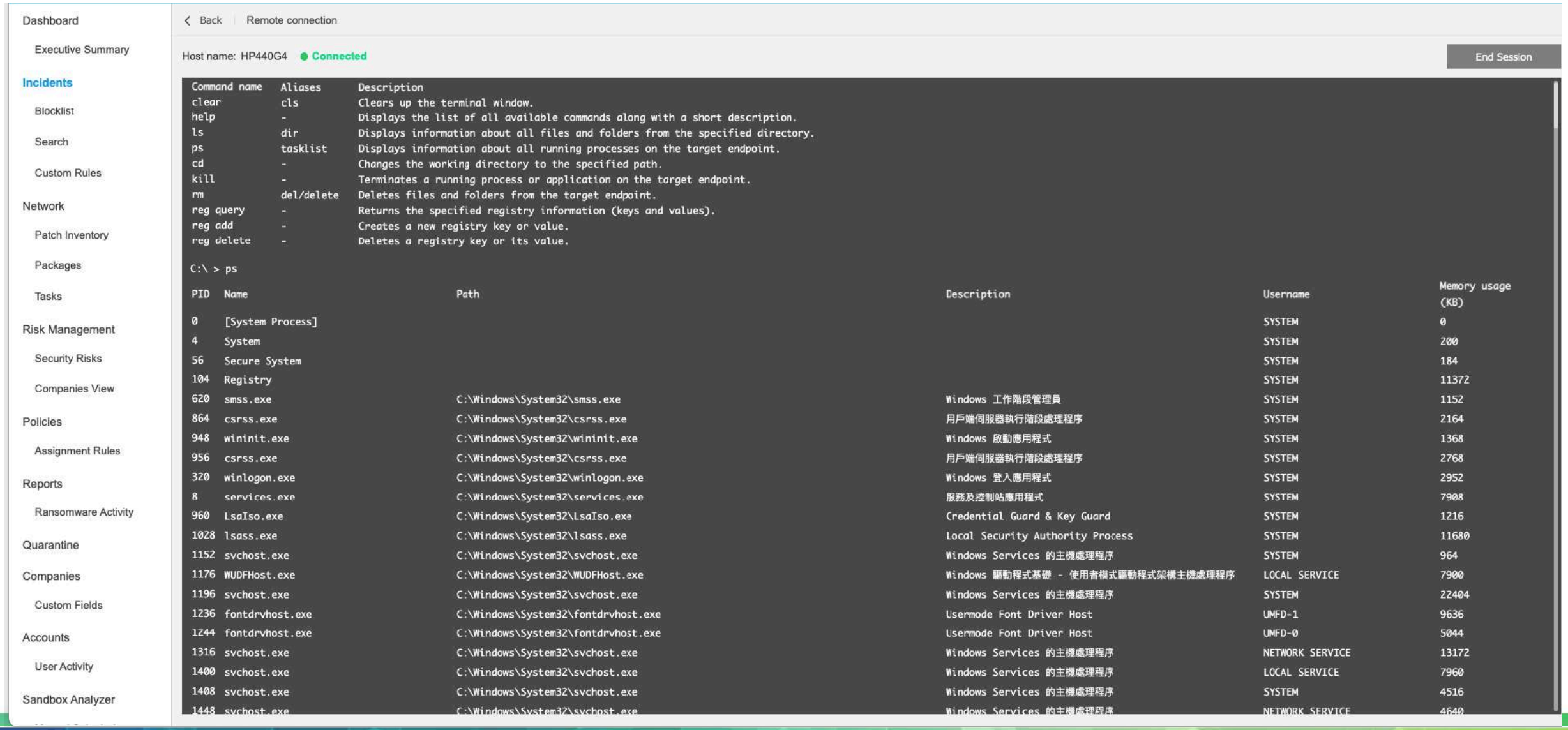
Procedure Examples

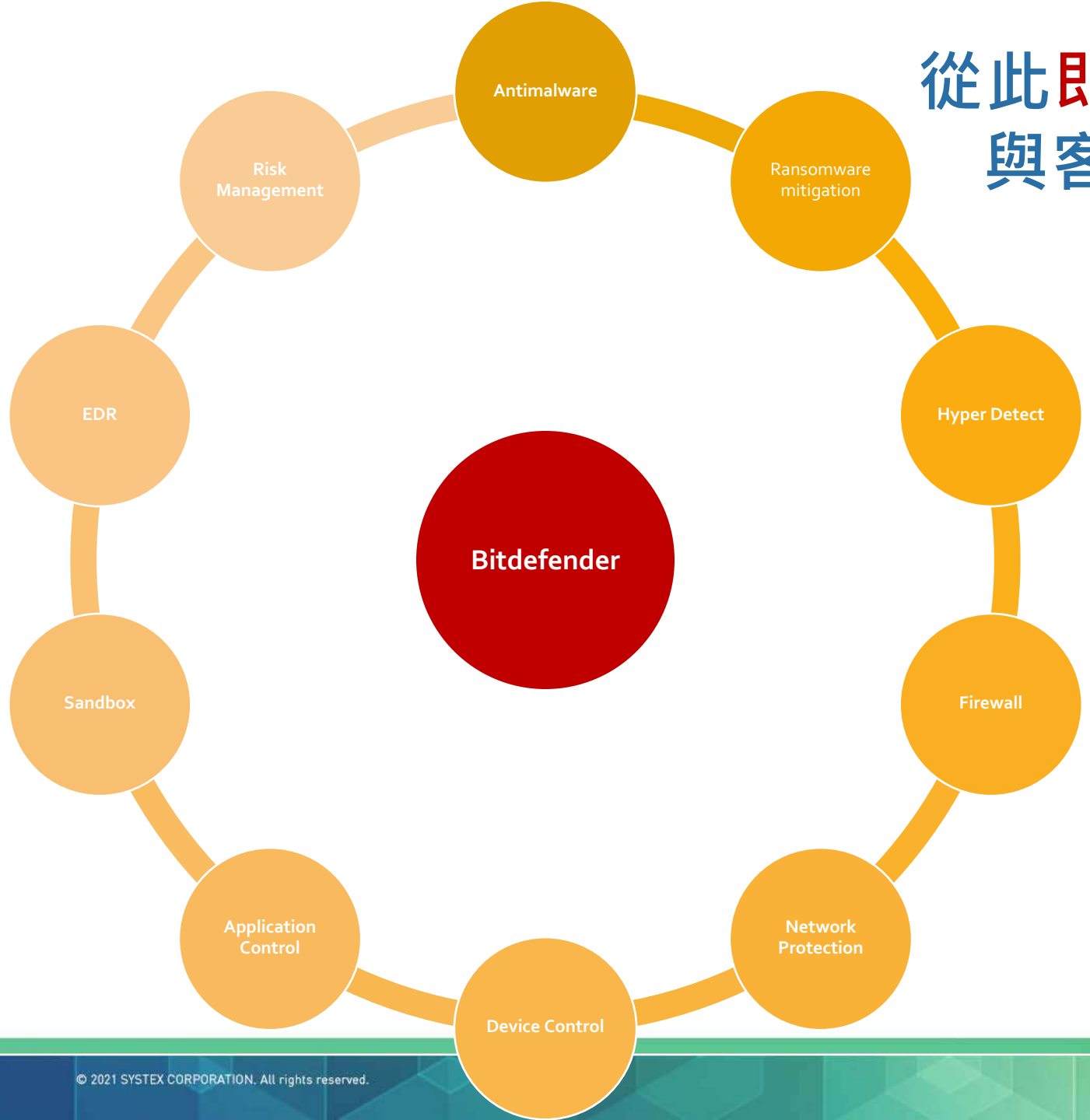
Name	Description
APT41	APT41 used BITSAdmin to download and install payloads.[8]
BITSAdmin	BITSAdmin can be used to create BITS Jobs to launch a malicious process.[9]
Cobalt Strike	Cobalt Strike can download a hosted "beacon" payload using BITSAdmin.[10]
JPIN	A JPIN variant downloads the backdoor payload via the BITS service.[11]
Leviathan	Leviathan has used BITSAdmin to download additional tools.[12]
Patchwork	Patchwork has used BITS jobs to download malicious payloads.[13]
UBoatRAT	UBoatRAT takes advantage of the /SetNotifyCmdLine option in BITSAdmin to ensure it stays running on a system to maintain persistence.[7]

單一平台即刻救援



即刻救援Remote connection





從此即刻救援，不再相見恨晚
與客戶共同持續營運發展資安力

- 資安防護規劃
- 資安鑑識
- 資安教育訓練
- 攻防演練
- 7*24監控
- 顧問服務

我會找到毒，並且把你清除!!

SYSTEX

Data Software **Orchestration**

Thank You