

# 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**<sup>®</sup>  
WWW.BITDEFENDER.COM

# 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

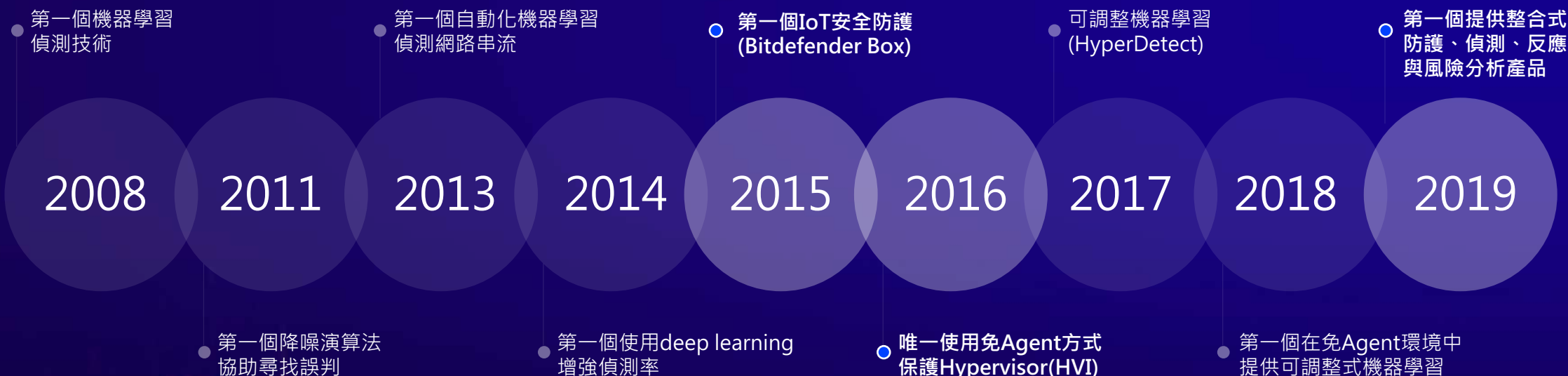
專業的技术研發公司

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

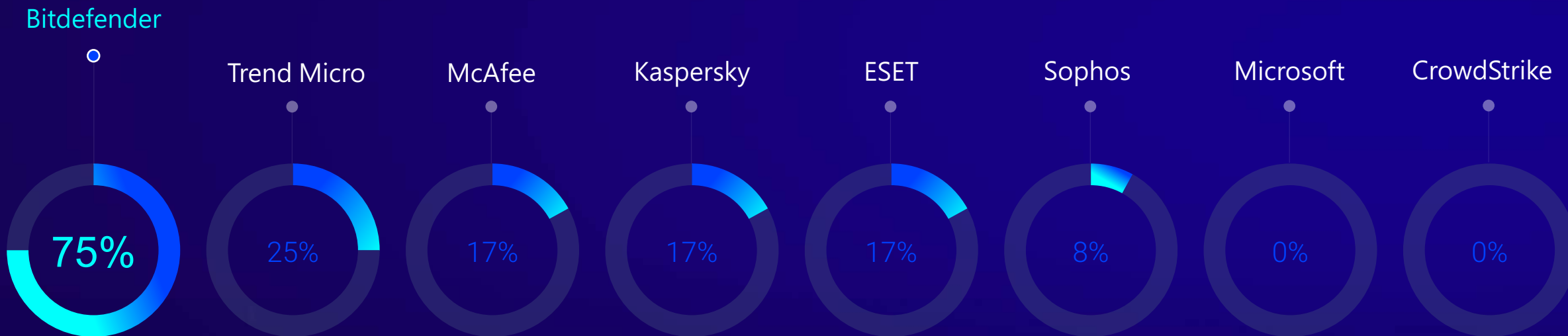
# 業界公認技術創新的領先者

專利得獎技術為38%的資安供應商採用



# 無可匹敵的攻擊防禦能力

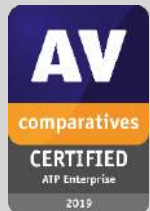
2018 & 2019 AV comparatives公正第三方測式中，獲得最多 #1 排名



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



“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

## 全球第三方資安分析 & 評測單位公認



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



SPEEDWAY MOTORSPORTS, INC.

esurance®



## PARTNERING AGAINST CYBER CRIME



FBI



Department of Justice



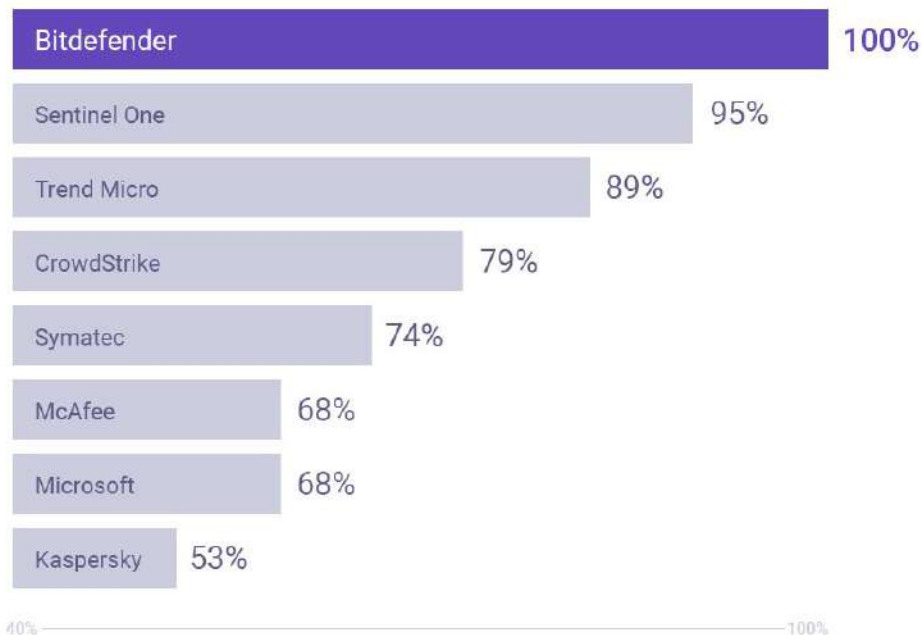
## TRUSTED BY

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, tactics and general detection, the most relevant ones for mid-sized organisations and MSPs, that are looking for processed EDR data.

For more info: <https://attacker.vals.mitre.org/APT29/results/bitdefender/>

MITRE | ATT&CK®



# OEM Technology Partnerships

Bitdefender

Support

My Account

For Home

For Business

For Partners

Company

Labs

## OEM Technology Partnerships

Proven by Countless Awards.  
Trusted by Hundreds of Technology partners

For the past 18 years, **our team has been creating award-winning technology** you can now easily integrate in your own products or services.

**Surprise your customers and leave your competition behind** with our top-of security solutions!

[CONTACT US](#)



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.



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 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.



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 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.



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 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 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 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 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.



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 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.

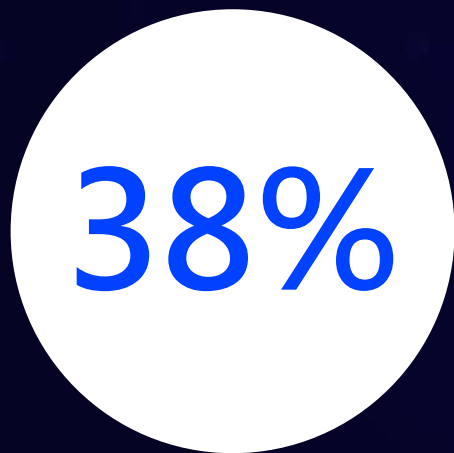
GRAVITYZONE™  
THE SECURITY PLATFORM FOR  
END-TO-END BREACH AVOIDANCE

“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®

10 Bitdefender®  
MARCH 24, 2021

# WHY BITDEFENDER



領先的技術提供者，  
38%以上的資安供應使用  
Bitdefender整合



無可比擬的攻擊防護。  
第三方評測長期#1



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、網路與雲端  
提供預防、偵測、反應與強化



## 進階端點安全

單一平台、單一agent提供  
預防、偵測、反應與風險分析



**Bitdefender®**  
**GRAVITYZONE**

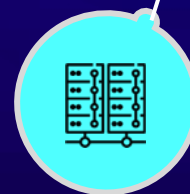
一個平台、一個Agent提供  
預防、偵測、反應與風險分析



## 資料中心 & 雲端



公有、私有、混合雲  
VDI, 軟體定義資料中心  
超融合架構



## 網路安全

IOT, NAS & MFT  
網路行為分析



# 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

## 強化 & 控制



## 預防



## 偵測 & 反應



全球威脅情資



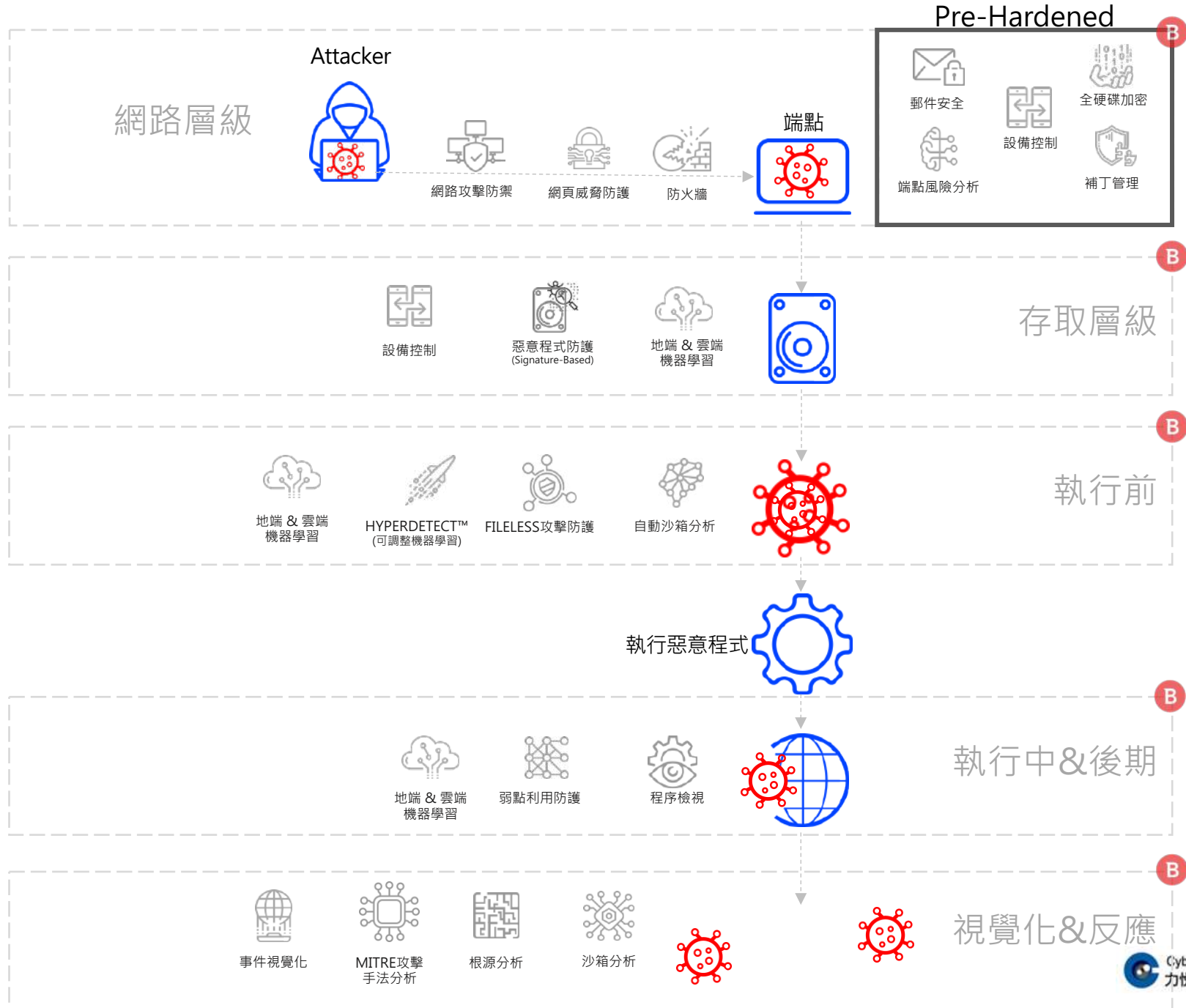
## 服務

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

# BITDEFENDER GRAVITYZONE®

@端點

# 最佳多層次保護



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

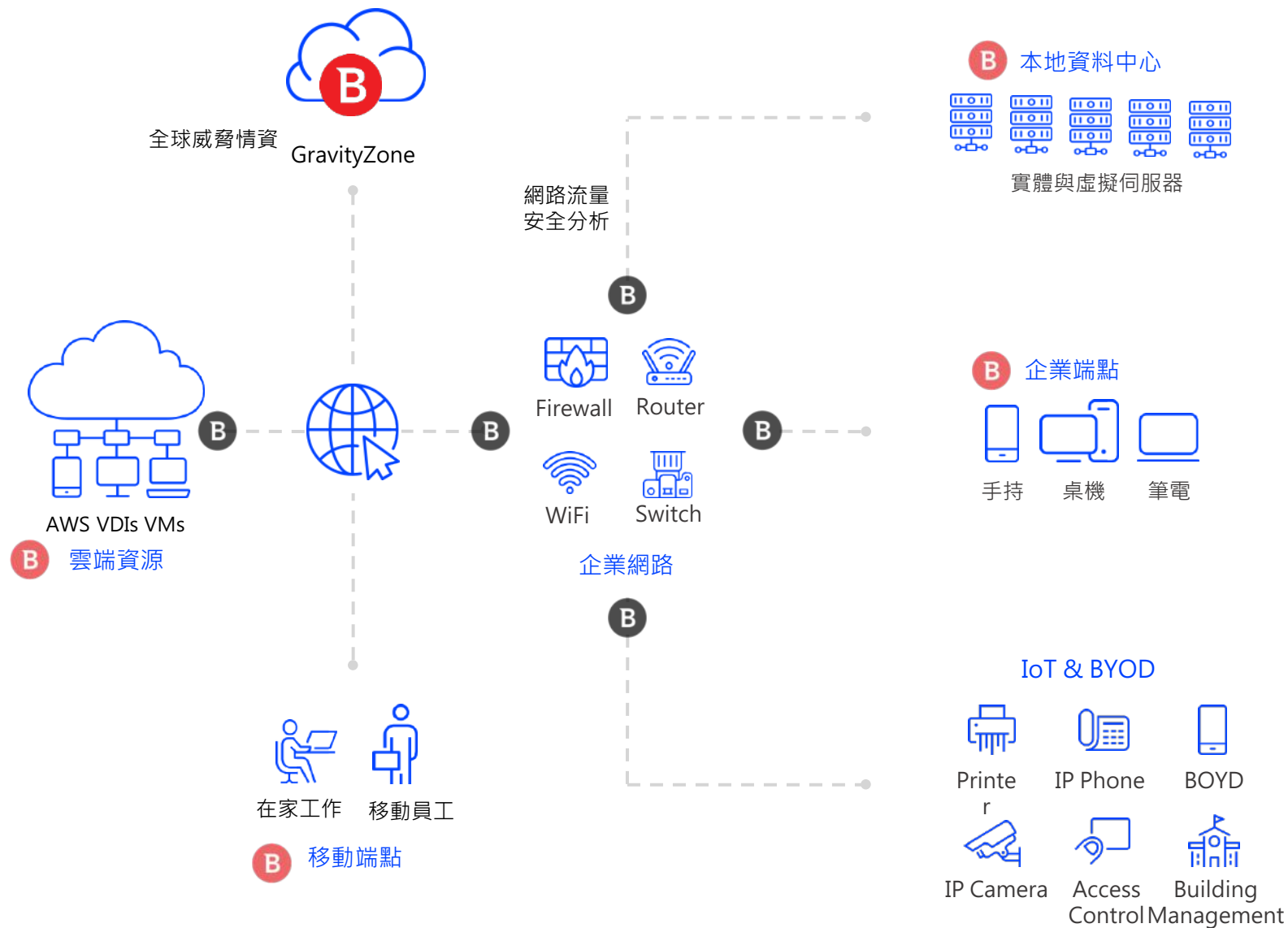
# BITDEFENDER GRAVITYZONE®

@網路



# Bitdefender ULTRA & NTSA 整合式平台效益

參考架構



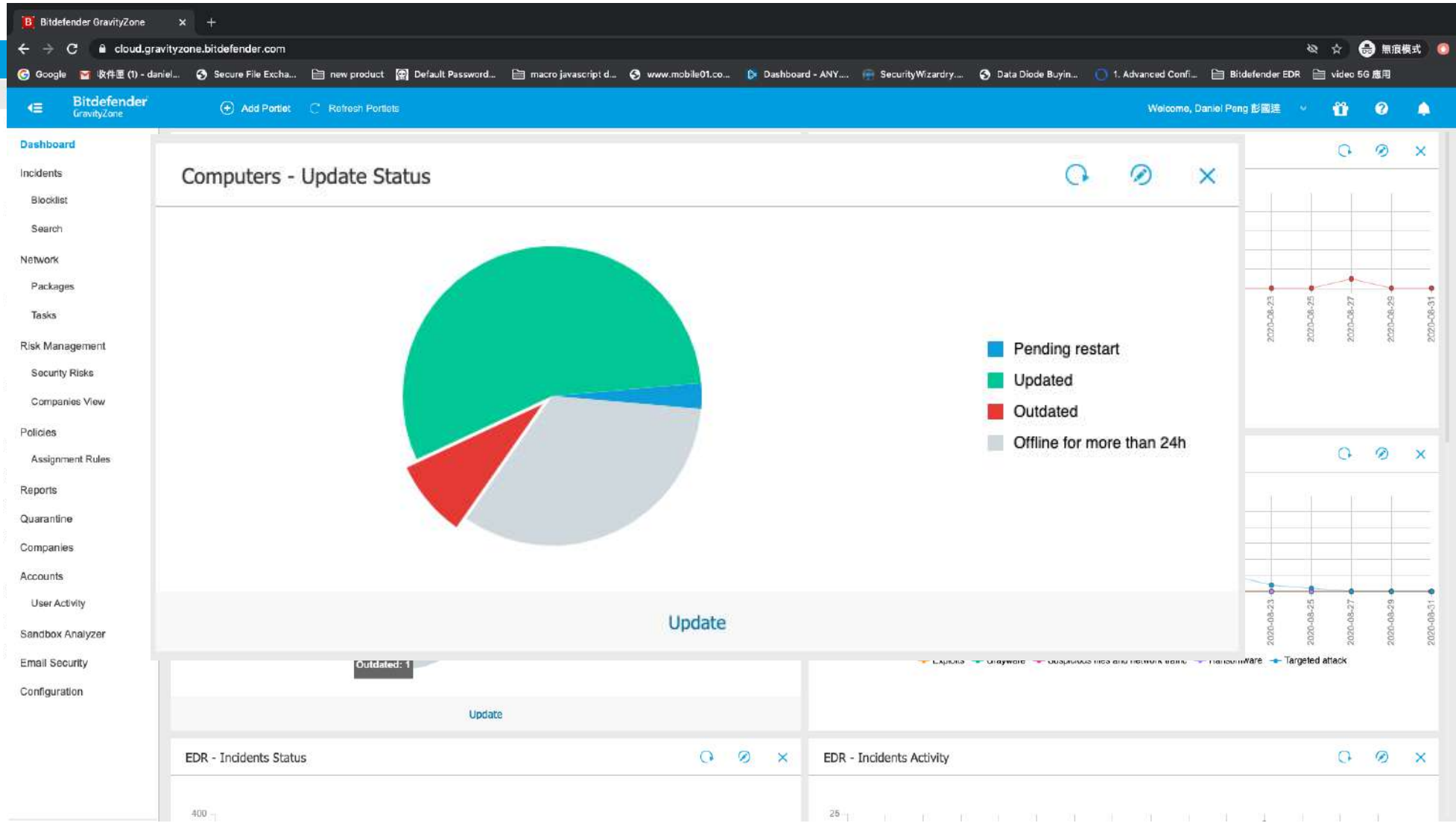
# BITDEFENDER GRAVITYZONE®

@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





# 完整遠端管理

隔離&控制  
Scan for IOC  
一般管理

The screenshot displays a management interface for a device named 'JESSICA'. A context menu is open, listing various management actions. The 'Tasks' menu item is selected, revealing a sub-menu with the following options: Scan, Scan for IOC, Risk scan, Patch Scan, Patch Install, Exchange Scan, Install, Repair client, Upgrade client, Uninstall client, Update client, Reconfigure Client, Restart machine, Network Discovery, and Update Security Server. Below the menu, the device's status is shown as 'Online'.

Infrastructure:	Computers and Groups
Group:	Endpoint
State:	Online



# 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

Search Get Started

registry.key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Pniumj AND registry.value: DataPath AND registry.operation: WRITE OR registry.operation: READ Search ☆

[Favorite Searches](#) 03 Jun 2020 03:02:00 to 01 Sep 2020 23:59:59 Cyberview\_local

GET STARTED WITH YOUR INVESTIGATION

The search is intended to help you through the analysis of incident data, collected in the GravityZone security events repository during the last 90 days. You can use the predefined search options below, or enter your own query to find out details about incidents. To learn more about GravityZone query language, check the [Syntax Help](#).

**PROCESS**

- Investigate unusual cmd.exe spawning by other processes.

**FILE**

- Identify payload masquerading as a legitimate Windows System Binary.

**NETWORK**

- Check for suspicious Remote Desktop Protocol (RDP) connections.

**REGISTRY**

- Search for Possible Remote Access Tool (RAT) activity.

**MALWARE DETECTIONS**

- Processes whose names are confusingly similar to those of critical system processes are likely to be malicious.
- Identify detected exploits that are potentially still active on endpoints.

**MITRE TECHNIQUES**

- Search for obfuscated files or information using ATT&CK TTP ID.
- Search for traces of credential dumping using ATT&CK technique naming.

**SUSPICIOUS ACTIVITY**

- Identify instances of running command shells, which may indicate threat actor activity.

23 Aug 2020, 00:02:55 **CV-ACTSRV** Event name: RemoteDesktopConnection Event description: New connection has been established on the remote desktop port.

First Page ← Page 1 of 18 → Last Page 100 ▼ 1723 items



# 風險分析

風控儀表  
組態錯誤  
應用程式弱點  
設備綜合風險  
人為風險

## Security Risks

Misconfigurations App Vulnerabilities **Human Risks** Devices Users

Ignore Risks

Human Risks	Severity	Vulnerable Users	Mitigation Type
<input type="checkbox"/> Search...	Choose...		Choose...
<input type="checkbox"/> Old User Password	Low (20%)	18	Manual

### Old User Password

Severity ● Low (20%)

Vulnerable Users 18

Risk Status Active

#### DETAILS

Verifies if the user has not changed the login password for the account (local or domain) for more than 30 days.

#### MITIGATIONS / USER ACTIONS

Change the login password for the local / domain account at least every 30 days.

Ignore Risk

View Users

MAKAYLA2	<span style="color: red;">●</span> High (86%)	95	0	Work
VOTIRO148	<span style="color: red;">●</span> High (86%)	83	0	Serve
WS2016	<span style="color: red;">●</span> High (86%)	85	0	Serve
SAM	<span style="color: red;">●</span> High (86%)	94	0	Work

16 items | FIRST PAGE < 1 of 1 > LAST PAGE | Show 20

Secure logon	+
UAC insecure	+
Store Domain Credentials	+
Insecure guest logon	-



# 其它重要功能

設備控管  
網站過濾  
防火牆&IDS

**Settings**

Protection level: Ruleset, known files and allow

Create aggressive rules

Create rules for applications blocked by IDS

Monitor process changes

Ignore signed processes

**Rules**

+ Add Up Down Export Import Delete

Priority	Name	Rule type	Network	Protocol	Permission
1	Incoming ICMP	Application	Home / Office,...	ICMP	Allow
2	Incoming ICMPV6	Application	Home / Office,...	IPv6-ICMP	Allow
3	Incoming Remote Desktop Connections	Connection	Home / Office,...	TCP	Allow
4	Sending Emails	Connection	Home / Office,...	TCP	Allow
5	Web Browsing HTTP	Application	Home / Office,...	TCP	Allow
6	Network Printing	Application	Home / Office,...	Any	Deny
7	Windows Explorer Traffic on FTP	Application	Home / Office,...	TCP	Deny
8	Windows Explorer Traffic on HTTP	Application	Home / Office,...	TCP	Deny

Photos/Videos: Allow Banks: Allow

Social Networks: Allow Business: Allow

Online Dating: Allow Computers and Software: Allow

IM: Allow Education: Allow

News: Allow Entertainment: Allow

Permanently: Block Government: Allow

Permission: Allowed

Save Cancel

# 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:

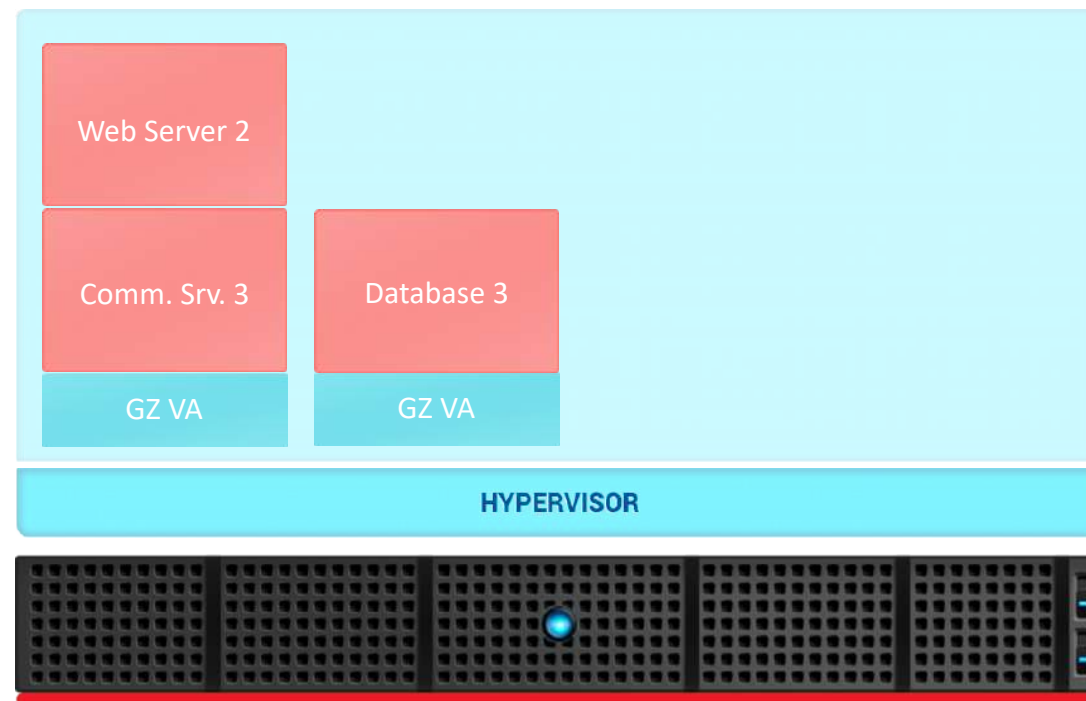
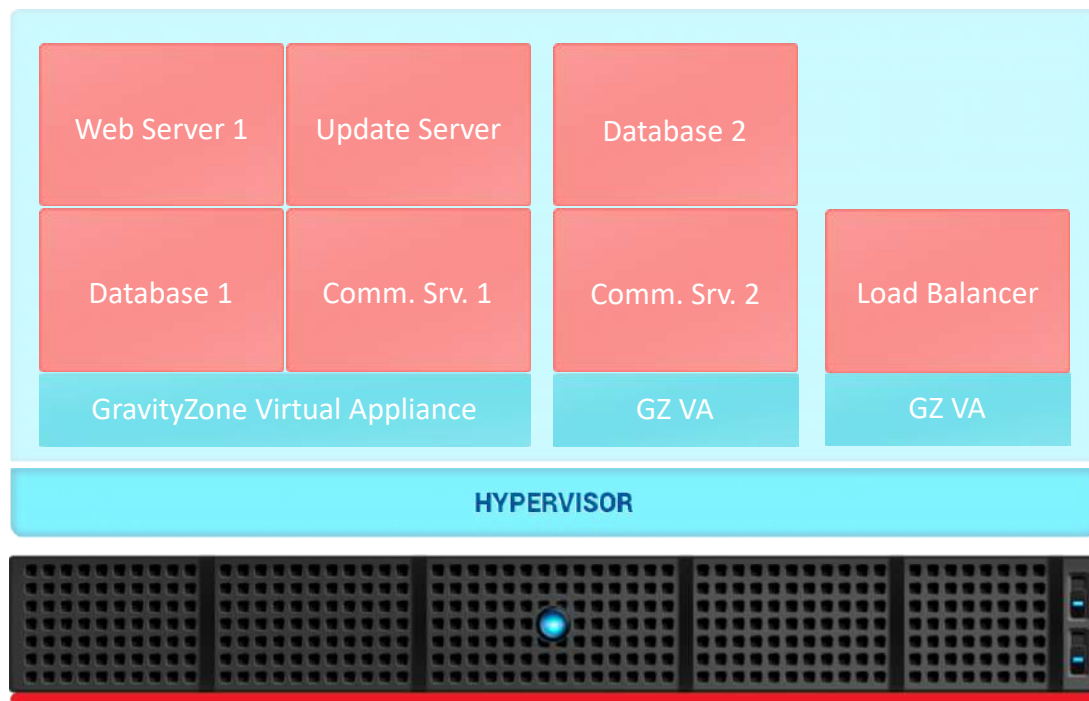
- Database(資料庫)
- Update Server(特徵碼更新服務)
- Web Server (Web Console 管理介面)
- Communication Server (端點聯繫溝通服務)

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

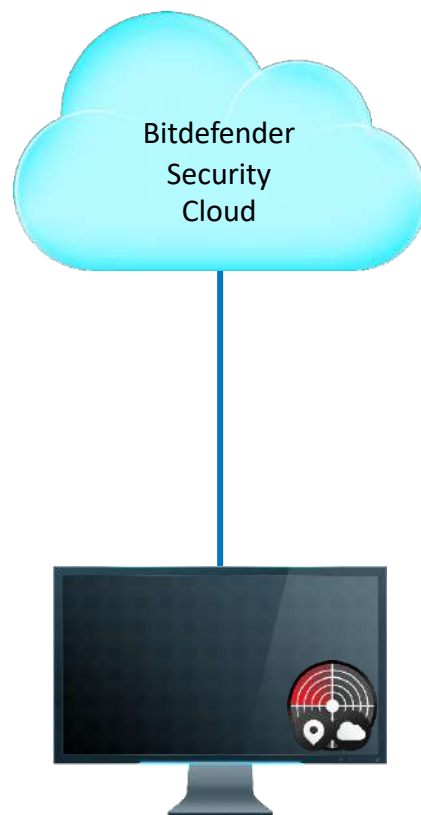


# 端點的安全防護

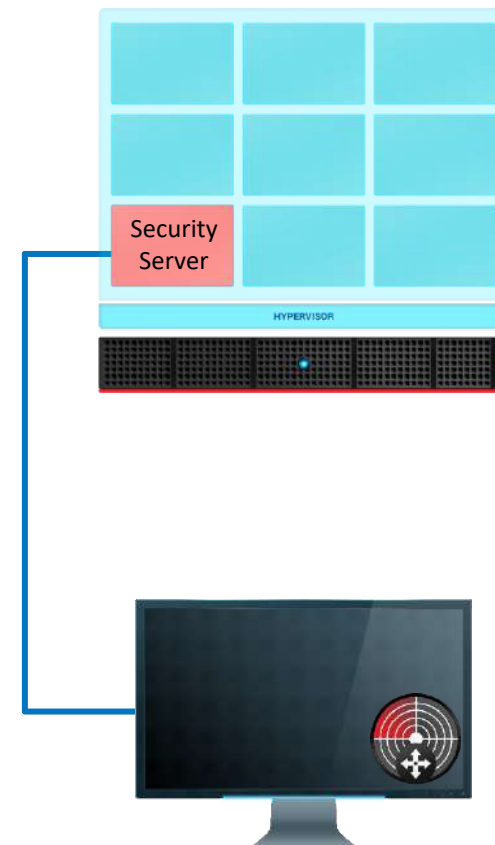
## 最棒的掃描引擎



本地(Local) Scan



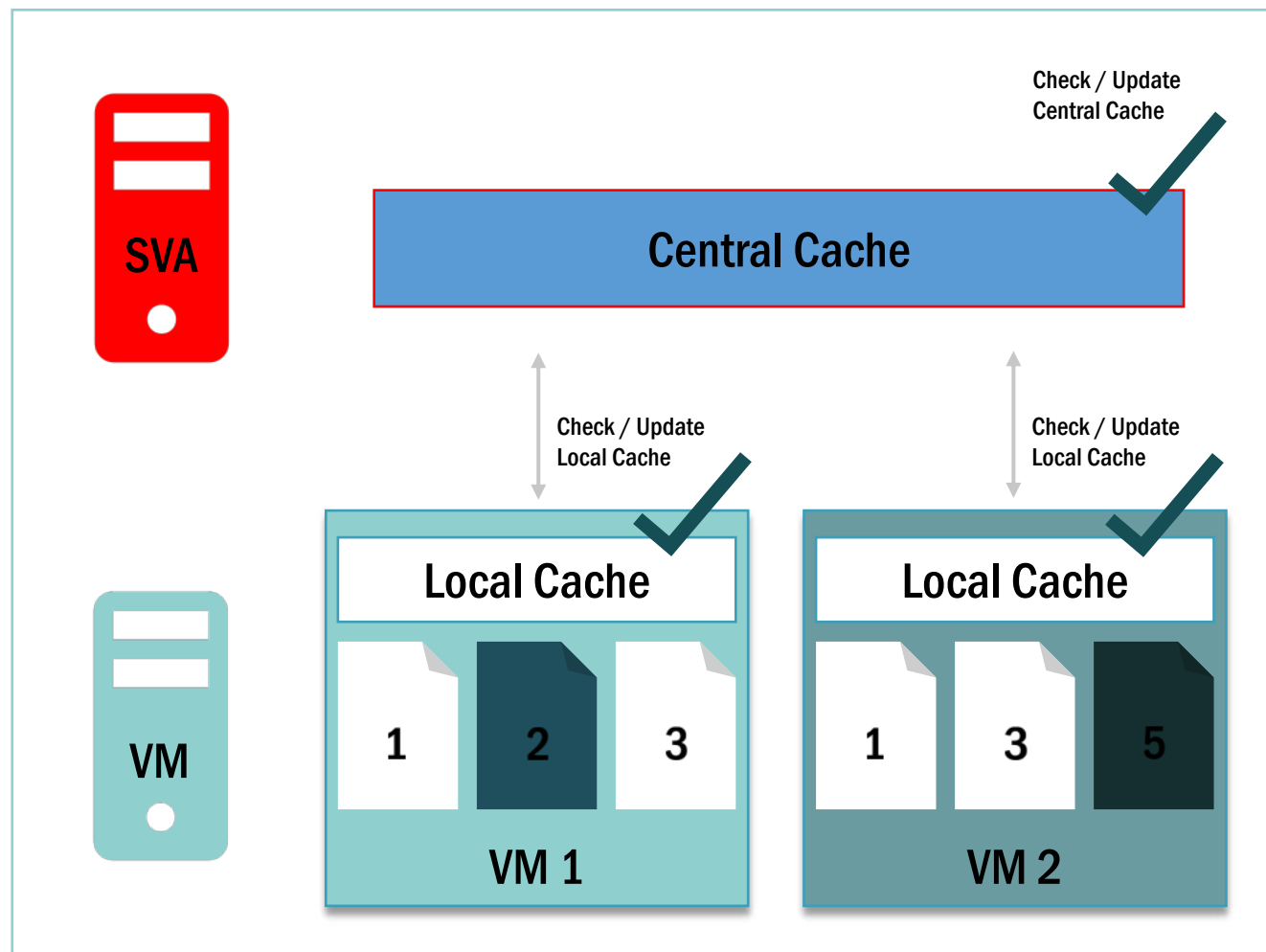
混合(Hybrid) Scan



中央(Central) Scan

# SECURITY SERVER

## PATENTED TWO-LEVEL CACHING



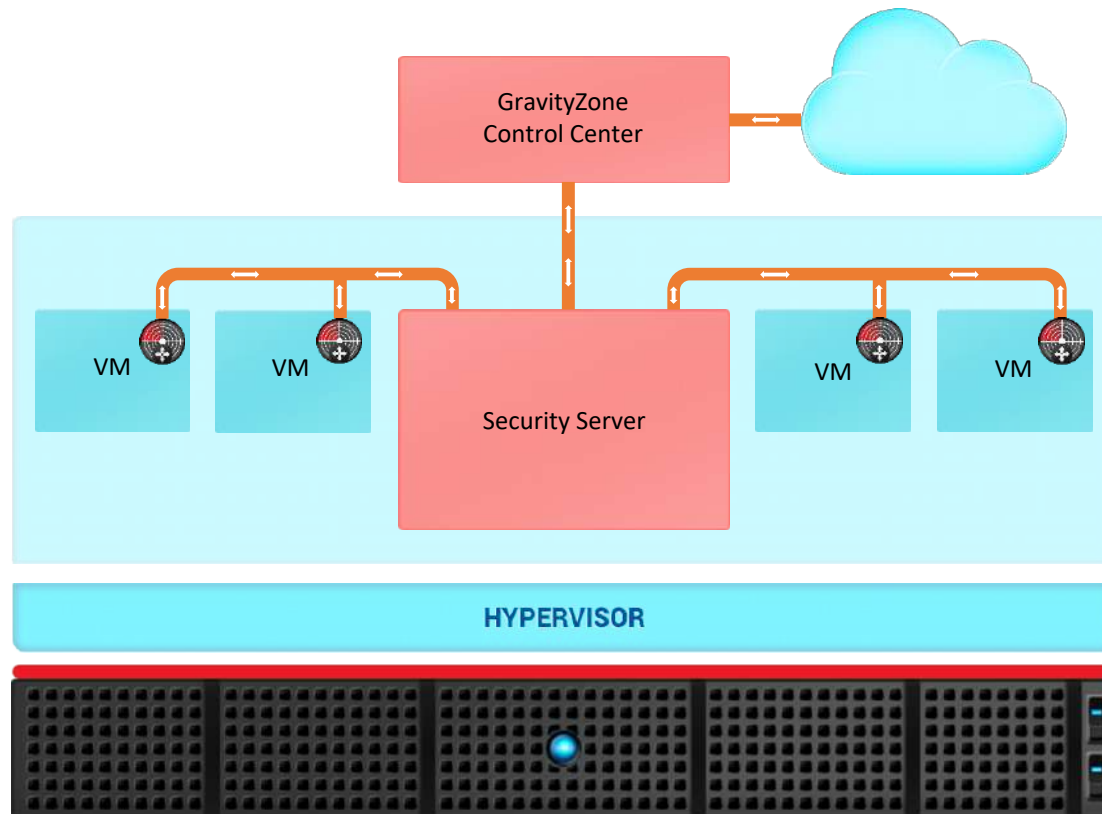
Two-level caching有效提高 VM(virtual machine) 和 SVA(security virtual appliance) 的反惡意軟件效率

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

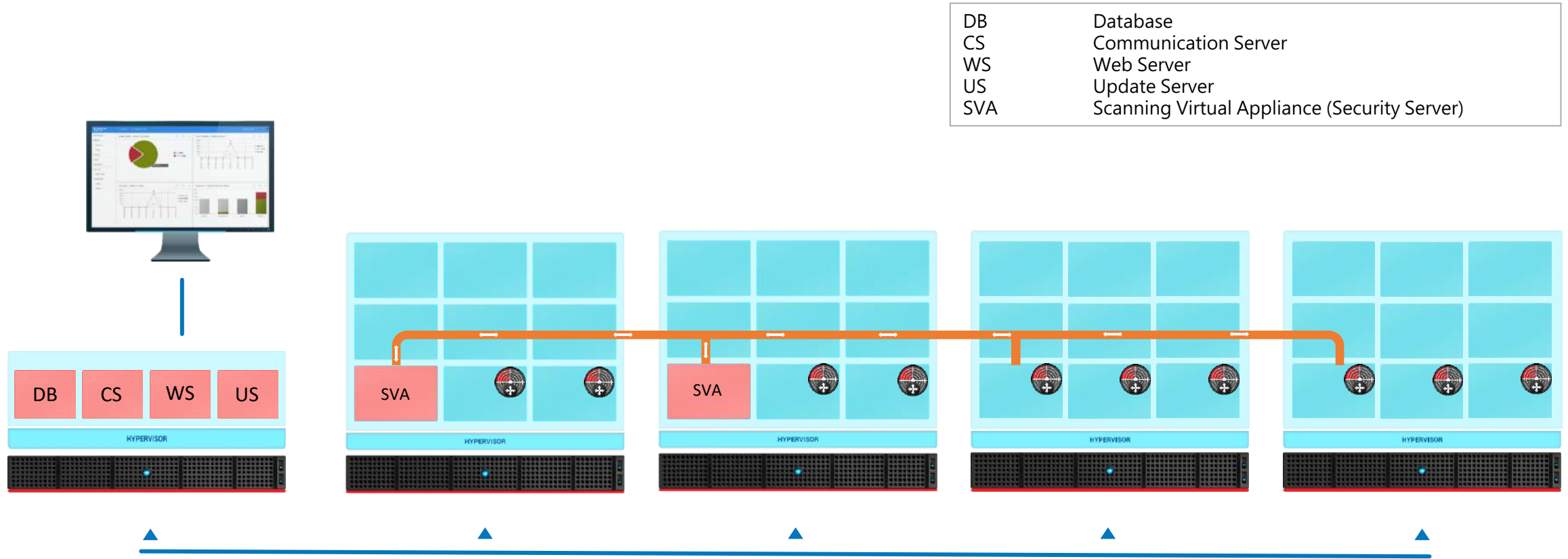
# SECURITY FOR VIRTUALIZED ENVIRONMENTS

## MULTIPLATFORM ARCHITECTURE (VMWARE)



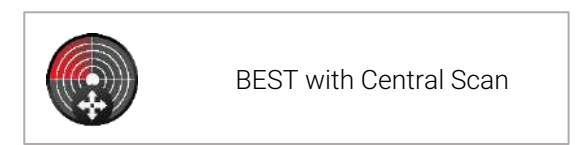
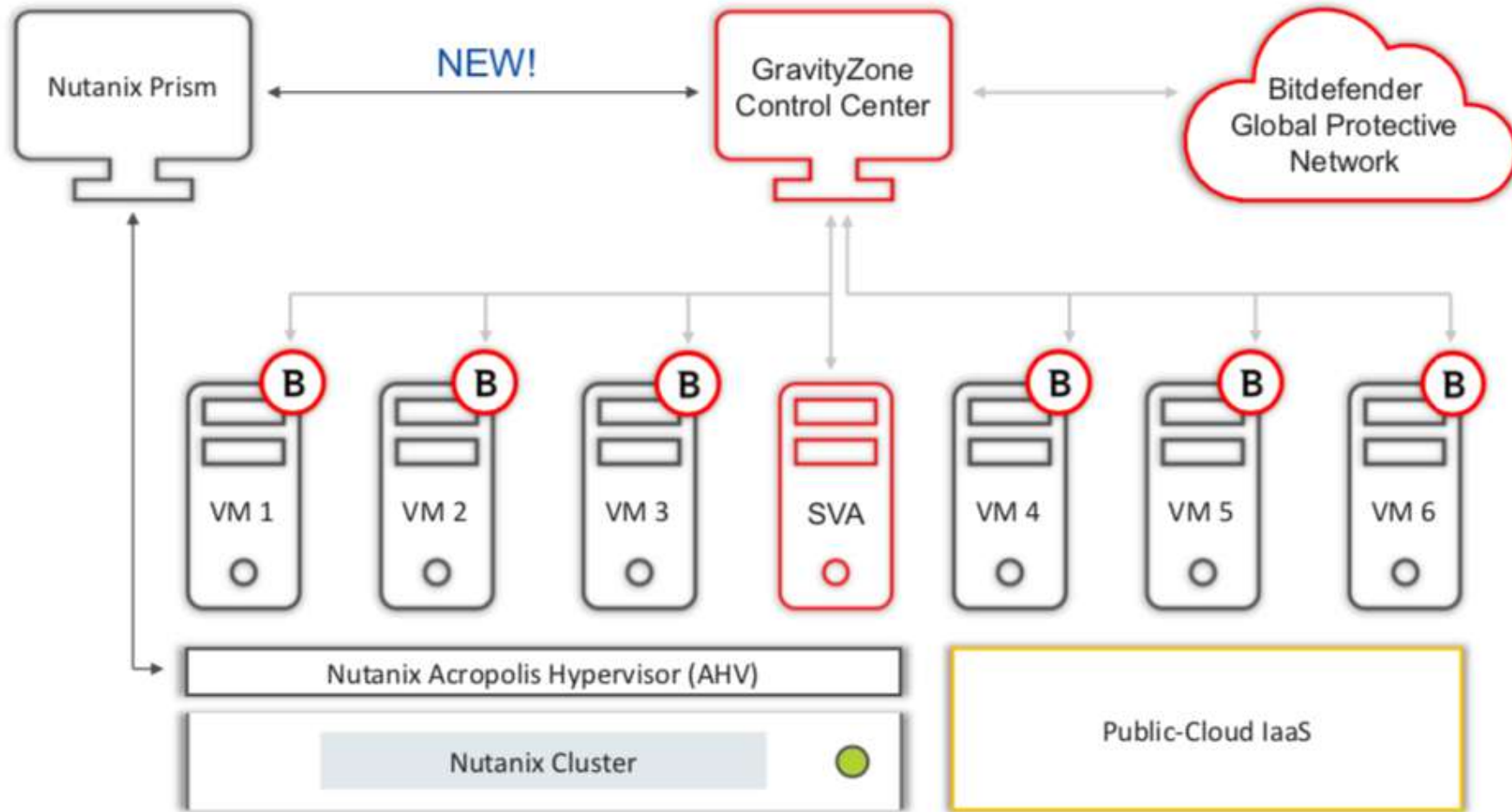
# SECURITY FOR VIRTUALIZED ENVIRONMENTS

## MULTIPLATFORM ARCHITECTURE (NUTANIX, CITRIX)

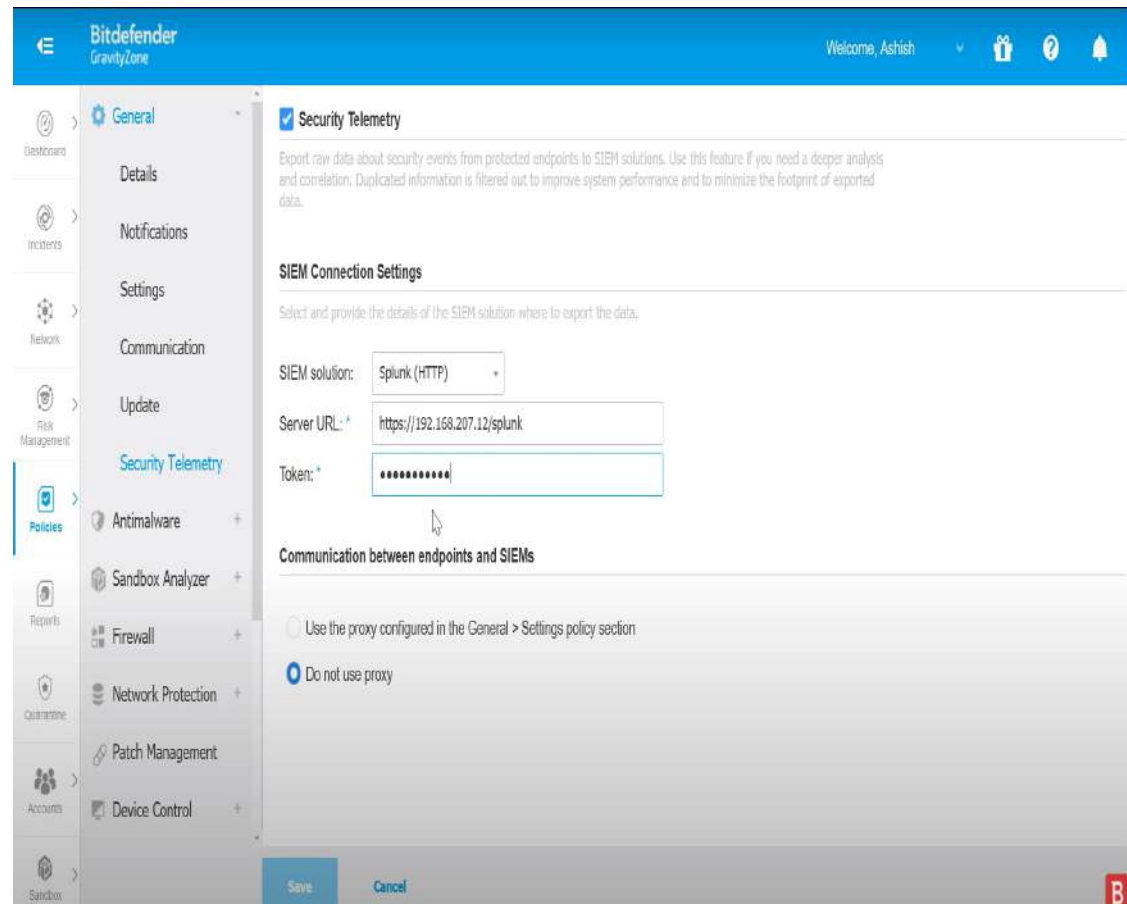
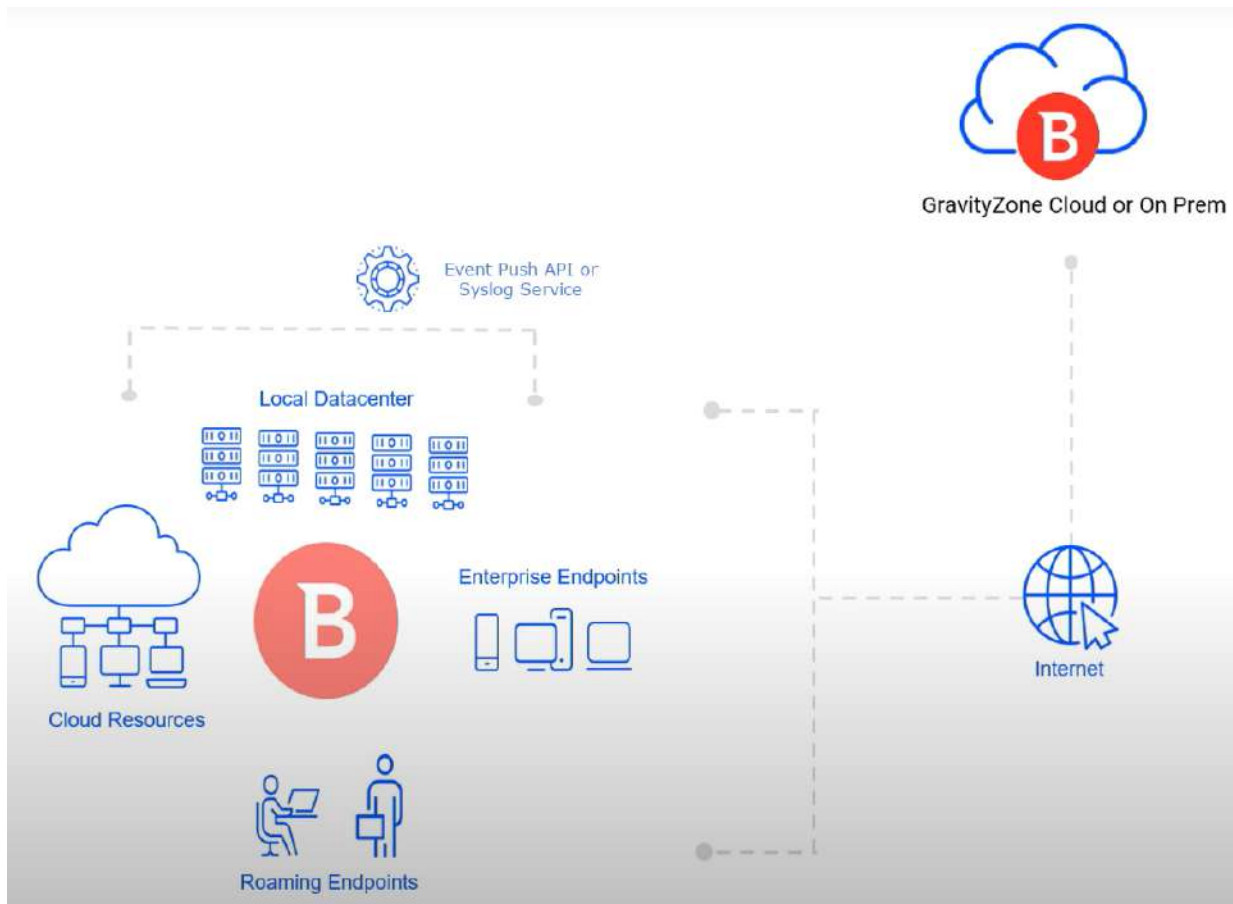


# SECURITY FOR VIRTUALIZED ENVIRONMENTS

整合虛擬機管理介面，AGENT自動佈建、回收



# 事件與RAW DATA轉發至SIEM



# RAW DATA支援搜尋(CLOUD版)地端使用SIEM

The screenshot displays the Bitdefender SIEM search interface. At the top, there is a search bar with the placeholder text "[Type your query...]" and a "Search" button. Below the search bar, a dropdown menu is open, showing a grid of search categories and their associated fields:

NETWORK	PROCESS	FILE	REGISTRY	DETECTIONS	OTHER
hostname	command_line	path	data	detection_name	API
URI	path	size	key	att&ck_technique_id	event_id
IP	pid	operation	operation	att&ck_technique	event_name
mac	size		type	actions_taken	hostname
port	user		value		exclusion_id
protocol					
bytes					
direction					

Below the search bar, there are several suggested queries organized into categories:

- PROCESS**
  - Investigate unusual cmd.exe spawning by other processes.
- FILE**
  - Identify payload masquerading as a legitimate Windows System Binary.
- NETWORK**
  - Check for suspicious Remote Desktop Protocol (RDP) connections.
- REGISTRY**
  - Search for Possible Remote Access Tool (RAT) activity.
- MALWARE DETECTIONS**
  - Processes whose names are confusingly similar to those of critical system processes are likely to be malicious.
  - Identify detected exploits that are potentially still active on endpoints.
- MITRE TECHNIQUES**
  - Search for obfuscated files or information using ATT&CK TTP ID.
  - Search for traces of credential dumping using ATT&CK technique naming.
- SUSPICIOUS ACTIVITY**
  - Identify instances of running command shells, which may indicate threat actor activity.



# 整合性(一)：全功能API

### API key ×

Enabled APIs:

<input type="checkbox"/> Companies API	<input type="checkbox"/> Reports API
<input type="checkbox"/> Licensing API	<input type="checkbox"/> Accounts API
<input type="checkbox"/> Packages API	<input type="checkbox"/> Incidents API
<input type="checkbox"/> Network API	<input type="checkbox"/> Quarantine API
<input type="checkbox"/> Integrations API	<input type="checkbox"/> Event Push Service API
<input type="checkbox"/> Policies API	

**Save** **Cancel**

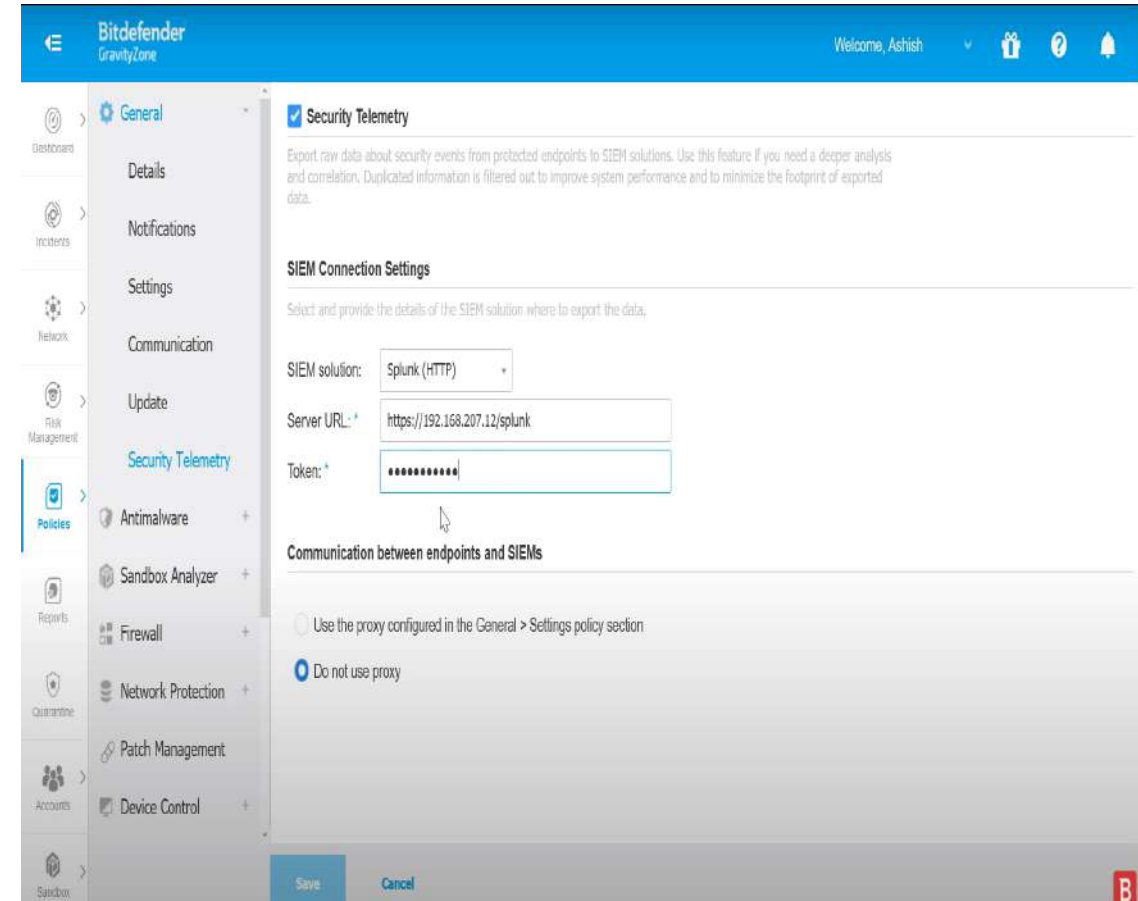
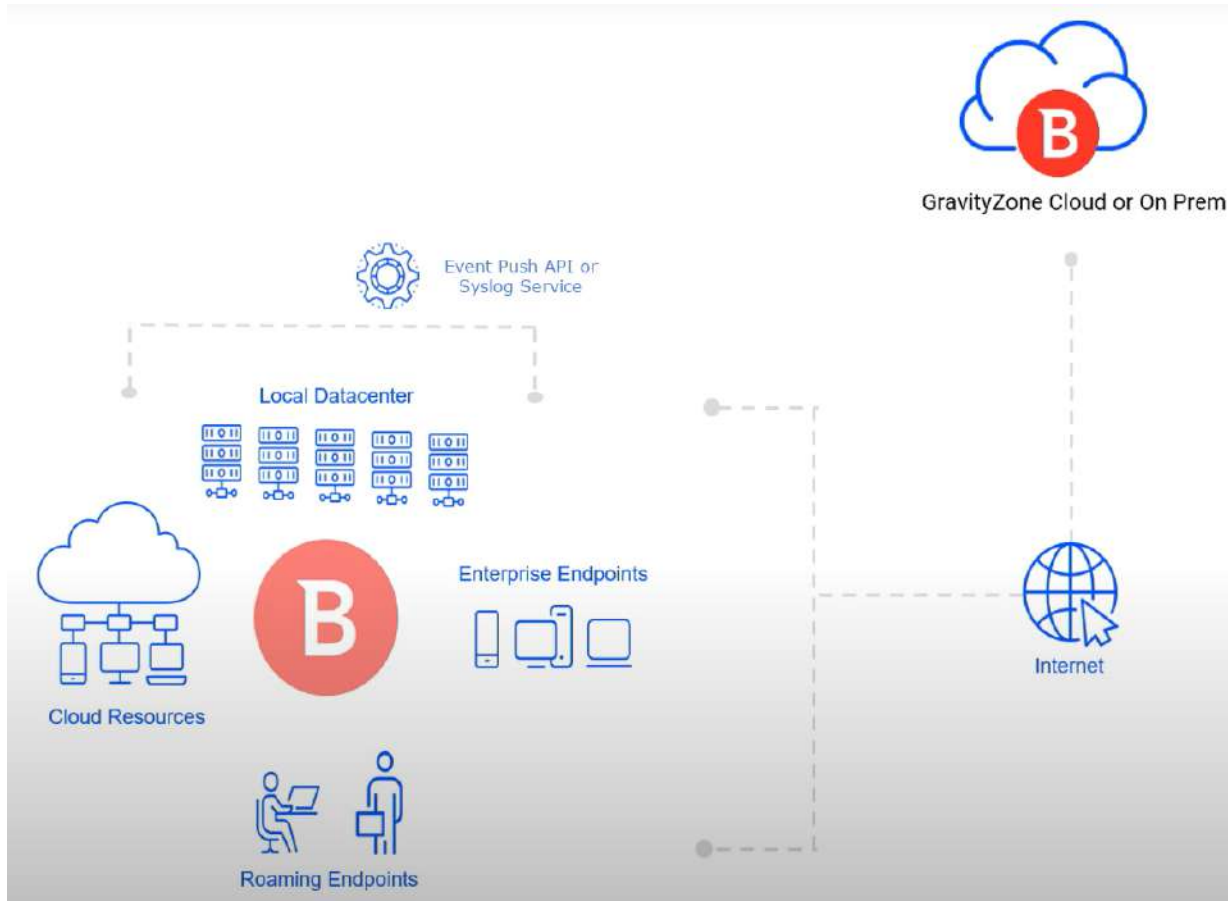
Access URL:

### API keys

+ Add - Delete ↻ Refresh

<input type="checkbox"/>	Key	Created
<input type="checkbox"/>	<input type="text" value="7323539349bbd88912301a57f98eaf64eae232e7827152"/>	Thu Jan 14 2021 21:48:31 GMT+0800 (台北標準時間)

# 整合性(二) : SIEM



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



Two-factor authentication

[New device?](#)

Cancel

Continue

## Configure single sign-on using SAML

For configuration details, refer to this [KB article](#).

GravityZone SAML metadata URL:

<https://gravityzone.bitdefender.com/sp/r>

Identity provider metadata URL:

-	Active Directory	<input type="checkbox"/>	ALLEN-WANG	Windows 7 Professional	192.168.1.207	4 hours ago	N/A
+	[redacted].local	<input type="checkbox"/>	ALVIN-CHENG	Windows 7 Professional	192.168.2.154	Now	N/A
+	Computers and Groups	<input type="checkbox"/>	AMOS-CHEN2	Windows 7 Professional	192.168.1.26	Now	N/A
+	Deleted	<input type="checkbox"/>	AMY-CHANG	Windows 7 Professional	192.168.1.155	Now	N/A

# Q&A

# THANK YOU!

# 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@SYSTEMX.COM](mailto:HANKLIN@SYSTEMX.COM)

**SYSTEMX**

Data Software **Orchestration**

# 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

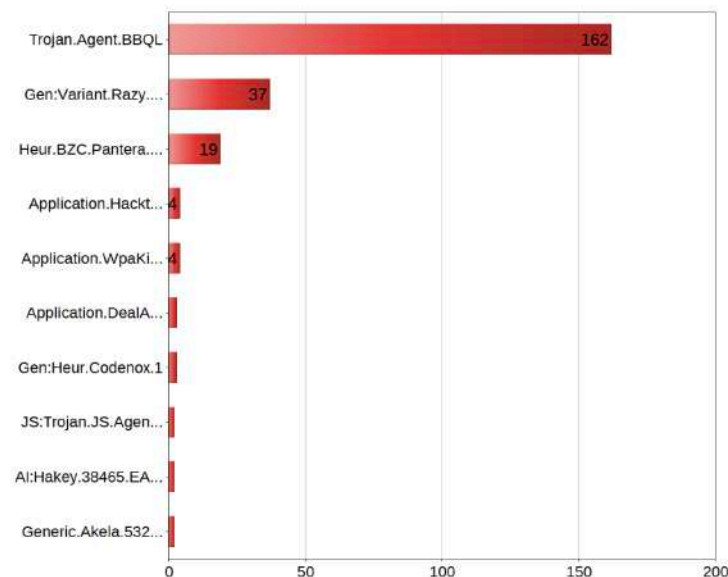


資料外洩使得  
詐騙集團勒索民眾

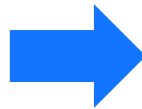
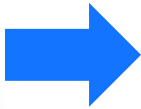
駭客

Computer	IP	File	Threat Name	Quarantined on	Action status
WS-138	192.168.15.135	D:\MSCV421B\application\disk1\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:38:42	None
WS-138	192.168.15.135	D:\LEK5-1-5-21-436374969-1580818891-1801674531-500\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:36:54	None
WS-138	192.168.15.135	D:\adll\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:38:46	None
SGI-PC	192.168.15.137	C:\Users\sgf\Downloads\FrostRose_Install_v10.2.0_thed\KMSpico_Install\KMSpico_setup.exe	Application.Hacktool.KMSpico	31 August 2020, 22:38:11	None
WS-138	192.168.15.135	D:\轉錄程式\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:34:37	None
WS-138	192.168.15.135	D:\存資料勿刪\本機螢幕 (D)\財務部\財務\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:38:18	None
WS-138	192.168.15.135	D:\STA_XP_2\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:33:04	None
WS-138	192.168.15.135	D:\存資料勿刪\本機螢幕 (D)\財務部\課員\螢幕截圖104\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:32:44	None
WS-138	192.168.15.135	D:\存資料勿刪\本機螢幕 (D)\財務部\好易\表格\備 案 用 中 文 表 格\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:32:43	None
WS-138	192.168.15.135	D:\備\本機螢幕 (D)\WebSoft\SU2108\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:30:41	None
WS-138	192.168.15.135	D:\k.dll	Gen:Variant.Razy.215296	31 August 2020, 22:30:23	None
WS-138	192.168.15.135	D:\存資料勿刪\本機螢幕 (D)\WebSoft\SU2008\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:30:18	None
WS-138	192.168.15.135	D:\MSCV421B\application\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:28:44	None
WS-138	192.168.15.135	D:\備\本機螢幕 (D)\VOISK\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:25:54	None
WS-138	192.168.15.135	D:\備\本機螢幕 (D)\VOISK\轉錄程式\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:25:54	None
WS-138	192.168.15.135	D:\備\本機螢幕 (D)\WINVISTA_XP_2\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:26:43	None
WS-138	192.168.15.135	D:\存資料勿刪\本機螢幕 (D)\VOISK\轉錄程式\pk.dll	Gen:Variant.Razy.215296	31 August 2020, 22:24:36	None

企業



# 實戰案例二



APT32代號：海上蓮花OceanLotus

漏洞



Threat Name	Date
cr4m20v5r0000gn/T/com.microsoft.Outlook/Outlook Temp/nm[oWX6].pdf	VB:Trojan.Valyria.3153 Jul 20, 2020 at 16:44
cr4m20v5r0000gn/T/com.microsoft.Outlook/Outlook Temp/nm[0T17].pdf	VB:Trojan.Valyria.3153 Jul 20, 2020 at 16:19
cr4m20v5r0000gn/T/com.microsoft.Outlook/Outlook Temp/nm[eWRu]...	VB:Trojan.Valyria.3153 Jul 20, 2020 at 16:19
cr4m20v5r0000gn/T/com.microsoft.Outlook/Outlook Temp/nm[2BwX].pdf	VB:Trojan.Valyria.3153 Jul 20, 2020 at 16:19
cr4m20v5r0000gn/T/com.microsoft.Outlook/Outlook Temp/nm[oHBW]...	VB:Trojan.Valyria.3153 Jul 15, 2020 at 23:22
cr4m20v5r0000gn/T/com.microsoft.Outlook/Outlook Temp/nm[nBqR].pdf	VB:Trojan.Valyria.3153 Jul 15, 2020 at 23:21
cr4m20v5r0000gn/T/com.microsoft.Outlook/Outlook Temp/nm[IOJF].pdf	VB:Trojan.Valyria.3153 Jul 15, 2020 at 23:21
cr4m20v5r0000gn/T/com.microsoft.Outlook/Outlook Temp/nm[AzFL].pdf	VB:Trojan.Valyria.3153 Jul 15, 2020 at 23:20

# 預防



# 各項模組的整合

## 偵測 & 反應



# 實戰案例三

Bitdefender GravityZone interface showing an incident investigation. The interface includes a sidebar with navigation options, a main content area with filters and endpoints, and a right-hand panel with alerts and investigation details.

**Filters Panel (Red Box):**

- Critical Path
- Endpoint: 1
- Process: 1
- Domain: 20
- Registry: 21

**Endpoints Table:**

Endpoint	Number of requests	First Accessed
A	6	10 February 2021, 00:15:10
B	2	03 March 2021, 00:54:20
C	4	10 February 2021, 00:15:10

**Alerts Panel (Right):**

- ALERTS**
- 1 DOMAIN DETECTED AS **MALWARE** BY ANALYSIS
- Exploit.PentestingTool.HTTP.3
- Network Attack Defense has detected a potential breach in your network, caused by **system**.
- Detected By: Network Attack Defe...
- Detected on: 03 Mar 2021, 00:54
- Severity: High

**Investigation Panel (Right):**

- INVESTIGATION**
- NETWORK ACTIVITY
- 3 endpoints | First Seen: 10 Feb 2021, 00:15
- REMEDIATION**
- ACTIONS TAKEN
- Process killed (auto)
- PREVENT
- Add URL as exception
- RECOMMENDED STEPS
- We recommend you take the following steps to mitigate this incident
- Exploit.PentestingTool.HTTP.3
- 1. Make sure all the endpoints in your network are protected and update the security solution on all of

# 實戰案例三

**Bitdefender GravityZone**

Dashboard | Executive Summary | Incidents | Blocklist | Search | Custom Rules | Network | Patch Inventory | Packages | Tasks | Risk Management | Security Risks | Companies View | Policies | Assignment Rules | Reports | Ransomware Activity | Quarantine | Companies | Custom Fields | Accounts | User Activity

Back | #1681 Blocked | Date: 03 Mar 2021, 19:52:00 | Status: Open | Incident Trigger: https://nice%2... | Endpoint: [redacted]

Graph | Events

All | Alerts | System events

03 Mar 2021, 00:54:20  
JERRYCHEN5F1-Z4  
192.168.8.117

Event name: Exploit.PentestingTool.HTTP.3 | Event description: Network Attack Defense has detected a potential breach in your network, caused by **system**.

Hide Details ^

Process | File | Network | Registry | Other

Uri: https://nice%20ports%2C/Tri%6Eity.bt%2ebak?

03 Mar 2021, 00:54:20  
JERRYCHEN5F1-Z4  
192.168.8.117

Event name: Exploit.PentestingTool.HTTP.3 | Event description: Network Attack Defense has detected a potential breach in your network, caused by **system**.

Hide Details ^

Process | File | Network | Registry | Other

Pid: 4

First Page | Page 1 of 1 | Last Page 100

2 items

# 實戰案例四

**Bitdefender GravityZone**

Dashboard | Executive Summary | Incidents | Blocklist | Search | Custom Rules | Network | Patch Inventory | Packages | Tasks | Risk Management | Security Risks | Companies View | Policies | Assignment Rules | Reports | Ransomware Activity | Quarantine | Companies | Custom Fields | Accounts | User Activity

Back | #777 Blocked | Date: 03 Mar 2021, 18:00:38 | Status: Open | Incident Trigger: bitsadmin.exe(...)

Filters: Critical Path | Endpoint: 1 | Process: 30 | File: 8 | Domain: 5 | Registry: 5

Graph | Events

wininit.exe (648)  
1. Executed  
services.exe (848)  
5. Executed  
svchost.exe (2140)  
40. Executed  
cmd.exe (14848)  
41. Executed  
bitsadmin.exe (2444)

Alerts: 3  
PROCESS DETECTED AS MALWARE BY ANALYSIS  
Heur.BZC.Leopard.10.10669288  
Antimalware has detected the bitsadmin.exe process during scanning, which executed a suspicious command line.  
Detected By: Fileless Attack Defense  
Detected on: 03 Mar 2021, 18:00  
Severity: High

Investigation: BITSAdminFileTransfer, BITSAdminUse

Network Presence: 2 endpoints | First Seen: 04 Nov 2020, 15:00

Further Analysis: Sandbox Analysis completed  
[View Sandbox Analyzer Report](#)  
[VirusTotal](#) | [Google](#)

Remediation: Denied access to file (auto)

# 實戰案例四

**Bitdefender GravityZone**

Dashboard  
Executive Summary

**Incidents**  
Blocklist  
Search  
Custom Rules

**Network**  
Patch Inventory  
Packages  
Tasks

**Risk Management**  
Security Risks  
Companies View

**Policies**  
Assignment Rules

**Reports**  
Ransomware Activity

**Quarantine**

**Companies**  
Custom Fields

**Accounts**  
User Activity

Back #777 Blocked Date 03 Mar 2021, 18:00:38 Status Open Incident Trigger bitsadmin.exe Endpoint

Filters  
Critical Path  
Endpoint 1  
Process 30  
File 8  
Domain 5  
Registry 5  
Search entities

Graph Events

wininit.exe (648)  
1. Executed  
services.exe (848)  
5. Executed  
svchost.exe (2140)  
40. Executed  
cmd.exe (14848)  
41. Executed  
bitsadmin.exe (2444)

bitsadmin.exe  
Process Execution

Add file to Blocklist Add file as exception

RECOMMENDED STEPS  
We recommend you take the following steps to mitigate this incident  
Heur.BZC.Leopard.10.10669288  
1. Make sure all the endpoints in your network are protected and update the security solution on all of them  
2. Perform a network-wide full-system scan.  
3. Check whether all operating systems in the network are up-to-date with the latest security  
Show more

**PROCESS INFO**

PROCESS EXECUTION DETAILS  
Process Name: bitsadmin.exe (ID:2...  
Command Line: /TRANSFER "Threat...  
User: NT AUTHORITY\SY...  
Execution Time: 03 NT AUTHORITY\SYSTEM

FILE INFO  
Hash: SHA256 | MD5  
Digitally Signed: No  
Size: 207.5 KB  
Path: c:\windows\system...



# 實戰案例四

The screenshot displays the Bitdefender GravityZone interface. The top navigation bar includes the Bitdefender logo, a home icon, a notification bell, and a search icon. The main content area is titled 'Incidents' and shows a list of alerts. The selected alert is from 03 Mar 2021, 18:00:20, with ID 507501N2 and IP 172.30.87.218. The event name is 'ATC.Malicious' and the description is 'Advanced Threat Control has labeled cmd.exe as a potential threat to your system.' A popup window titled 'ATT&CK Techniques' is open, listing 'Execution' techniques (Command-Line Interface, Scripting) and 'Defense Evasion' techniques (BITS Jobs, Process Injection, Scripting). Below the popup, the 'ATT&CK Techniques: Defense Evasion -BITS Jobs ... show all' link is highlighted. The bottom of the screen shows a pagination bar with 'Page 1 of 1' and 'Last Page 100'.

Bitdefender GravityZone

Dashboard

Executive Summary

Incidents

Blocklist

Search

Custom Rules

Network

Patch Inventory

Packages

Tasks

Risk Management

Security Risks

Companies View

Policies

Assignment Rules

Reports

Ransomware Activity

Quarantine

Companies

Custom Fields

Accounts

User Activity

Back | #777 Blocked | Date 03 Mar 2021, 18:00:38 | Status Open | Incident Trigger bitsadmin.exe(... | Endpoint

Graph | Events

All Alerts System events

03 Mar 2021, 18:00:20  
507501N2  
172.30.87.218

Event name: ATC.Malicious  
Event description: Advanced Threat Control has labeled cmd.exe as a potential threat to your system.

ATT&CK Techniques: Execution -Command-Line Interface

More Details

03 Mar 2021, 18:00:19  
507501N2  
172.30.87.218

Event name: CertUtil Process Execution  
Event description: CertUtil is a command-line utility that can be used to obtain certificate authority information and configure Certificate Services.

ATT&CK Techniques: Defense Evasion -BITS Jobs, Process Injection, Scripting

More Details

03 Mar 2021, 18:00:19  
507501N2  
172.30.87.218

Event name: Heur.BZC.Leopard.10.0DC6D056  
Event description: Heur.BZC.Leopard.10.0DC6D056 is a heuristic rule for detecting malware, which executed a suspicious command line.

ATT&CK Techniques: Defense Evasion -BITS Jobs, Process Injection, Scripting

More Details

03 Mar 2021, 18:00:17  
507501N2  
172.30.87.218

Event name: BITSAdminUse  
Event description: BitsAdmin process executed.

ATT&CK Techniques: Defense Evasion -BITS Jobs ... show all

More Details

03 Mar 2021, 18:00:17  
507501N2  
172.30.87.218

Event name: BITSAdminFileTransfer  
Event description: BitsAdmin was used to transfer a file.

ATT&CK Techniques: Execution -Command-Line Interface

More Details

First Page | Page 1 of 1 | Last Page 100

37 items

# Bitdefender與MITRE ATT&CK攻擊手法名稱一致

MITRE | ATT&CK

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search

Execution Persistence Account Manipulation BITS Jobs Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Browser Extensions Compromise Client Software Binary Create Account Create or Modify System Process Event Triggered Execution External Remote Services Hijack Execution Flow Implant Container Image Office Application Startup Pre-OS Boot Scheduled Task/Job Server Software Component Traffic Signaling Valid Accounts

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<sup>[2]</sup> and the BITSAdmin tool.<sup>[3]</sup>

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.<sup>[4]</sup><sup>[5]</sup><sup>[6]</sup> 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).<sup>[7]</sup><sup>[4]</sup>

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

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

# 單一平台即刻救援

The screenshot displays the Bitdefender GravityZone console interface. The top navigation bar includes the Bitdefender logo and user profile information. The left sidebar contains various management sections: Dashboard, Incidents, Network, Risk Management, Policies, Reports, Quarantine, Companies, Accounts, and Sandbox Analyzer. The main area shows an incident summary for endpoint HP440G4, including a status of 'Blocked', date '22 Feb 2021, 09:28:16', and status 'Open'. A network diagram below shows the endpoint's position within a corporate network structure. The right-hand panel is titled 'REMEDIATION' and contains the following sections:

- ACTIONS TAKEN:** No actions taken
- FIX & REMEDIATE:** Isolate host, Install patches, Remote connection
- DEVICE INFO:** ENDPOINT DETAILS including FQDN (hp440g4), IP (192.168.2.106), OS (Windows 10 Pro), Infrastructure (Computers and Groups), Group (Custom Groups), State (Online), Last seen (Online), and Active Policy (Direct Cloud Policy).
- PATCH INFORMATION:** Patch Management license not available, Last Checked (Never), Patch status (Unknown).

# 即刻救援 Remote connection

Dashboard

Executive Summary

Incidents

Blocklist

Search

Custom Rules

Network

Patch Inventory

Packages

Tasks

Risk Management

Security Risks

Companies View

Policies

Assignment Rules

Reports

Ransomware Activity

Quarantine

Companies

Custom Fields

Accounts

User Activity

Sandbox Analyzer

< Back | Remote connection

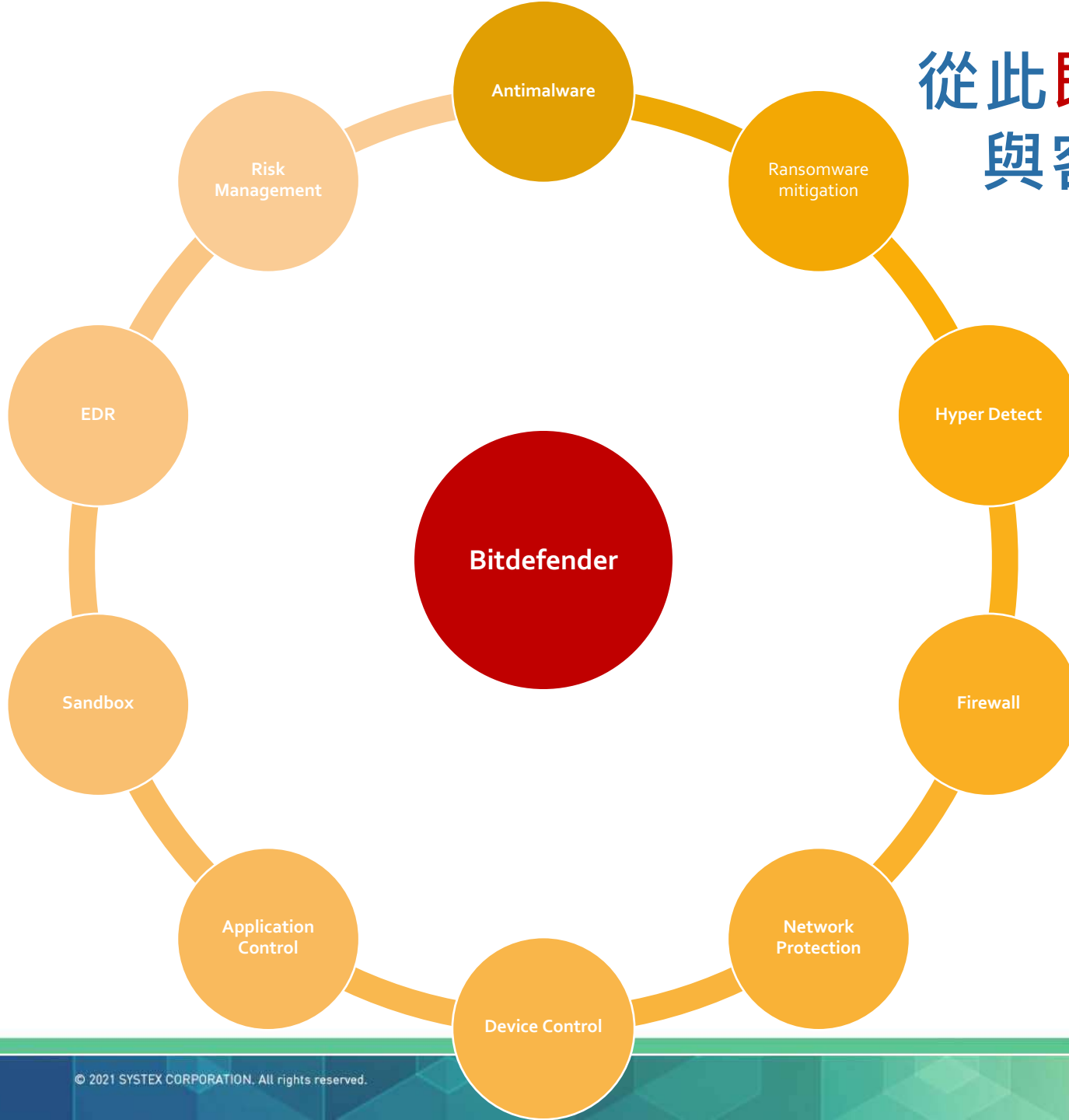
Host name: HP440G4 ● Connected End Session

Command name	Aliases	Description
clear	cls	Clears up the terminal window.
help	-	Displays the list of all available commands along with a short description.
ls	dir	Displays information about all files and folders from the specified directory.
ps	tasklist	Displays information about all running processes on the target endpoint.
cd	-	Changes the working directory to the specified path.
kill	-	Terminates a running process or application on the target endpoint.
rm	del/delete	Deletes files and folders from the target endpoint.
reg query	-	Returns the specified registry information (keys and values).
reg add	-	Creates a new registry key or value.
reg delete	-	Deletes a registry key or its value.

C:\> ps

PID	Name	Path	Description	Username	Memory usage (KB)
0	[System Process]			SYSTEM	0
4	System			SYSTEM	200
56	Secure System			SYSTEM	184
104	Registry			SYSTEM	11372
620	smss.exe	C:\Windows\System32\smss.exe	Windows 工作階段管理員	SYSTEM	1152
864	csrss.exe	C:\Windows\System32\csrss.exe	用戶端伺服器執行階段處理程序	SYSTEM	2164
948	wininit.exe	C:\Windows\System32\wininit.exe	Windows 啟動應用程式	SYSTEM	1368
956	csrss.exe	C:\Windows\System32\csrss.exe	用戶端伺服器執行階段處理程序	SYSTEM	2768
320	winlogon.exe	C:\Windows\System32\winlogon.exe	Windows 登入應用程式	SYSTEM	2952
8	services.exe	C:\Windows\System32\services.exe	服務及控制站應用程式	SYSTEM	7908
960	LsaIso.exe	C:\Windows\System32\LsaIso.exe	Credential Guard & Key Guard	SYSTEM	1216
1028	lsass.exe	C:\Windows\System32\lsass.exe	Local Security Authority Process	SYSTEM	11680
1152	svchost.exe	C:\Windows\System32\svchost.exe	Windows Services 的主機處理程序	SYSTEM	964
1176	WUDFHost.exe	C:\Windows\System32\WUDFHost.exe	Windows 驅動程式基礎 - 使用者模式驅動程式架構主機處理程序	LOCAL SERVICE	7900
1196	svchost.exe	C:\Windows\System32\svchost.exe	Windows Services 的主機處理程序	SYSTEM	22404
1236	fontdrvhost.exe	C:\Windows\System32\fontdrvhost.exe	Usermode Font Driver Host	UMFD-1	9636
1244	fontdrvhost.exe	C:\Windows\System32\fontdrvhost.exe	Usermode Font Driver Host	UMFD-0	5044
1316	svchost.exe	C:\Windows\System32\svchost.exe	Windows Services 的主機處理程序	NETWORK SERVICE	13172
1400	svchost.exe	C:\Windows\System32\svchost.exe	Windows Services 的主機處理程序	LOCAL SERVICE	7960
1408	svchost.exe	C:\Windows\System32\svchost.exe	Windows Services 的主機處理程序	SYSTEM	4516
1448	svchost.exe	C:\Windows\System32\svchost.exe	Windows Services 的主機處理程序	NETWORK SERVICE	4640

# 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!!



SYSTEMEX

Data Software **Orchestration**

**Thank You**