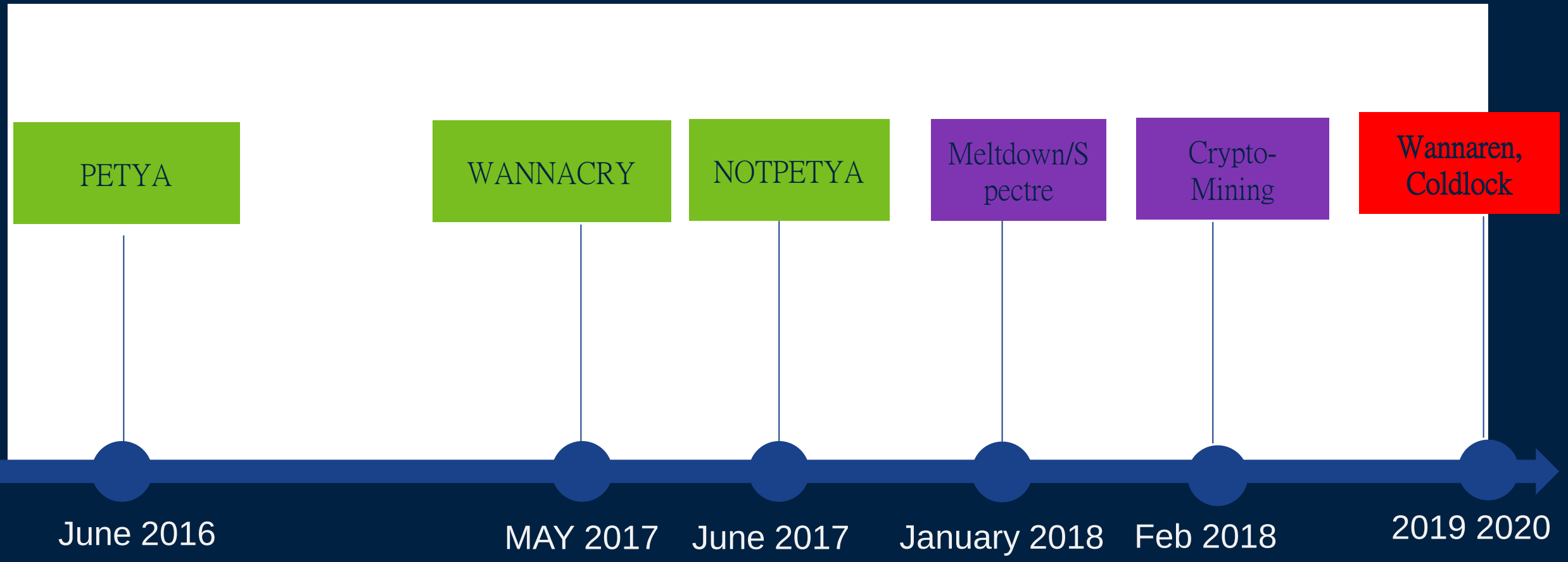
VMware Carbon Black
新世代端點防護-特殊威脅解決方案
助您阻擋先進攻擊

Luis Chang 張志淵

August 2020

vmware Confidential | ©2020 VMware, Inc.

勒索病毒越來越多TIMELINE



今年第一季勒索病毒跟去年比增加148%

vmware Carbon Black

Products Solutions Partners Resources Company Schedule a Demo

Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted

April 15, 2020 / PATRICK UPATHAM , JIM TREINEN

Cyber criminals often exploit fear and uncertainty during major world events by launching cyberattacks. These attacks are often performed with social engineering campaigns leveraging malicious emails that lure victims to install malware that steals financial data and other valuable personal information or, in some cases, turns a user's computer into a crypto mining zombie.

In light of the COVID-19 surge, we looked into attack data from the VMware Carbon Black Cloud to determine the shift to remote work, how cyber attackers have stepped up their campaigns, when these campaigns are being launched,

Subscribe

Enter Your Email Address

Subscribe

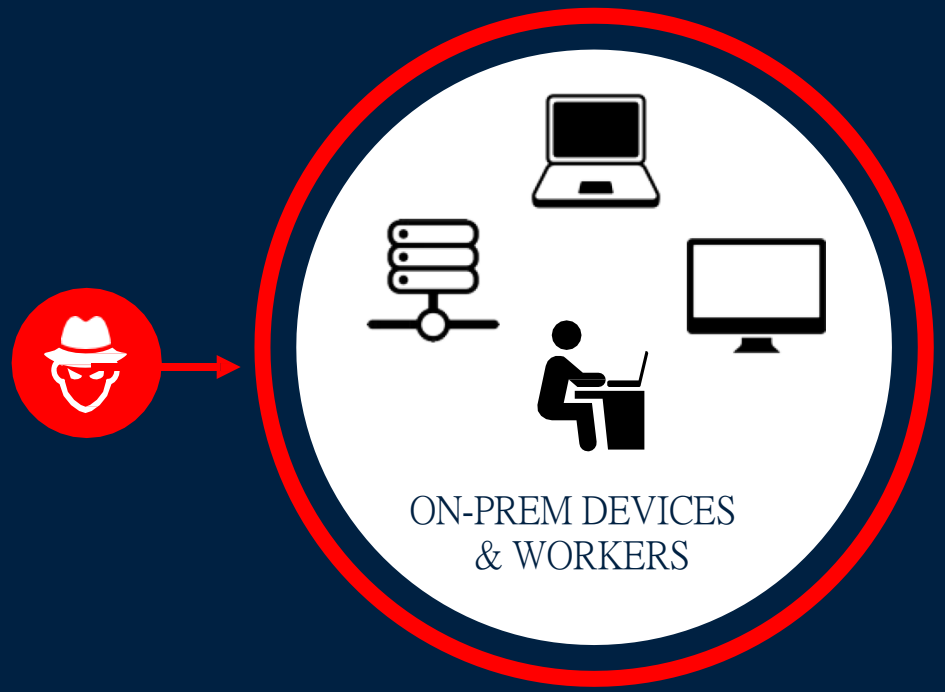
Latest Tweets

In 2008 Tom was appointed a commissioner on the Commission on Cyber Security for the 44th President of the United States.
Tom Kellermann is the Chief Cybersecurity Officer for Carbon Black Inc.

行政院資安處過去曾經做過統計，台灣公部門每個月遭受境外網路攻擊的次數，平均達 3,000 萬次，和歐洲國家一個月可能只有幾萬次相比，台灣受攻擊的頻率非常高。

行動化 & 雲端運算正在轉變對資訊安全的思維

Before
The Network Was the Perimeter



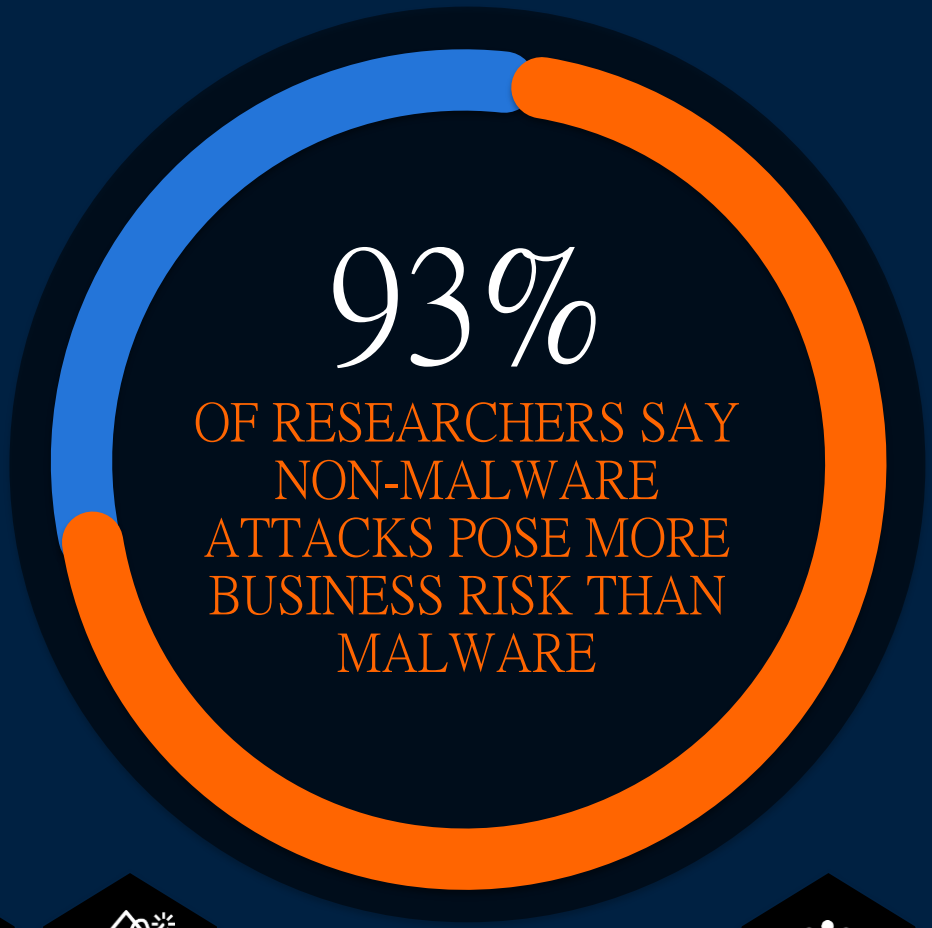
Today
The Endpoint Is the NEW Perimeter

vmware
Confidential | ©2020 VMware, Inc.

80% 的攻擊都是未知的, 防毒軟體只對20%攻擊有用

20%

OF BREACHES USE MALWARE



80%

OF BREACHES ARE NON-MALWARE

KNOWN | UNKNOWN | RANSOM | OBFUSCATED

MALWARE ATTACKS

MEMORY | MACROS | REMOTE LOGIN | POWERSHELL

NON-MALWARE ATTACKS

vmware
Confidential | ©2020 VMware, Inc.

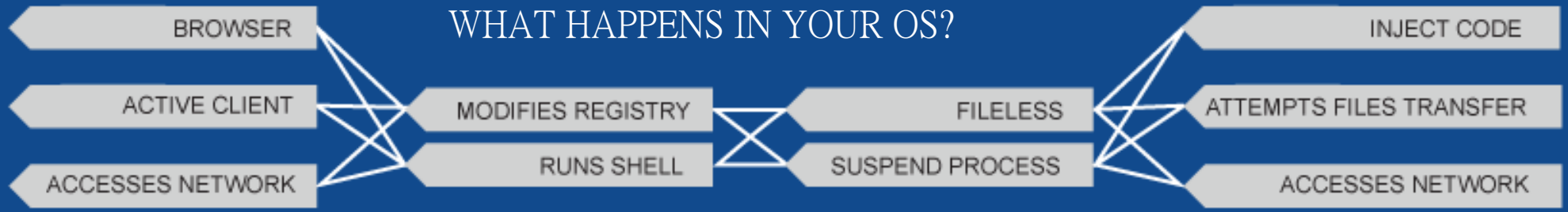
藏在正常行爲下的攻擊(資料盜取, 勒索病毒）

1

USE OF LEGITIMATE APPLICATIONS TO LAUNCH ATTACKS

2

WHAT HAPPENS IN YOUR OS?



3

AV and Machine Learning CANNOT STOP THIS

CB是端點安全市場領導者

MARKET-LEADING
DETECTION
& RESPONSE

.....

PRO-ACTIVE
THREAT HUNTING

.....

PURPOSE BUILT
FOR SOC/IR

80%+
Y/Y Growth

11,000+
Customers

20,000
Practitioners

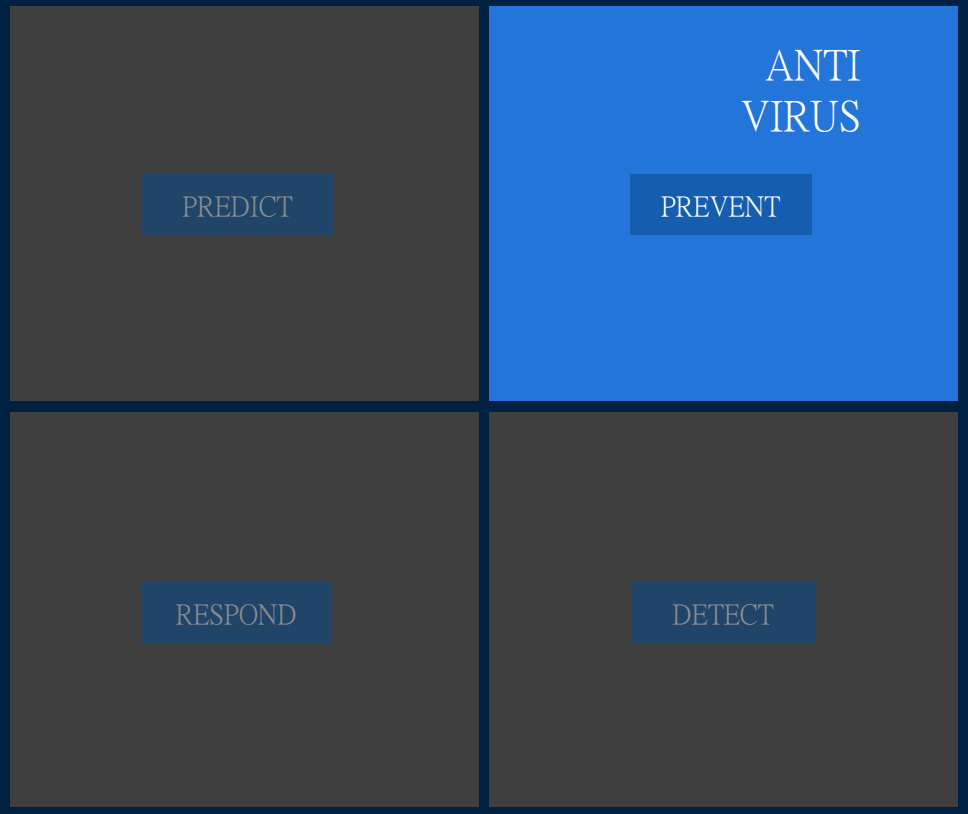
50
of Fortune 100

250+
IR/MSSPs

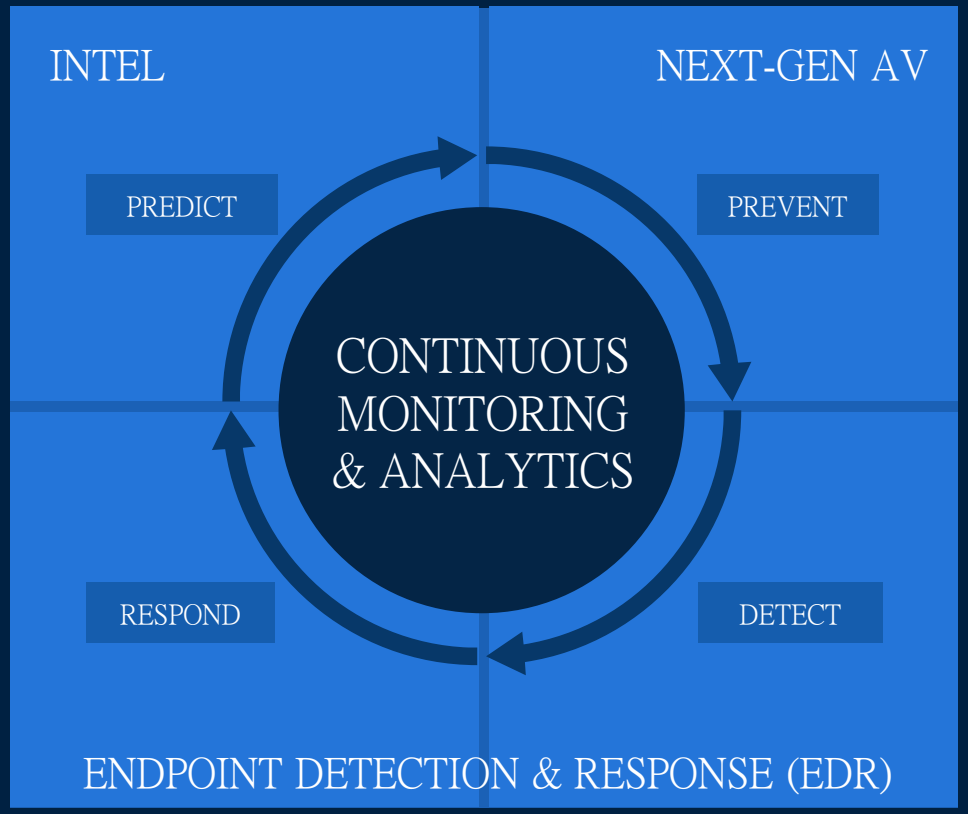
35M
Endpoints

Carbon Black 提供持續性的Cybersecurity監控

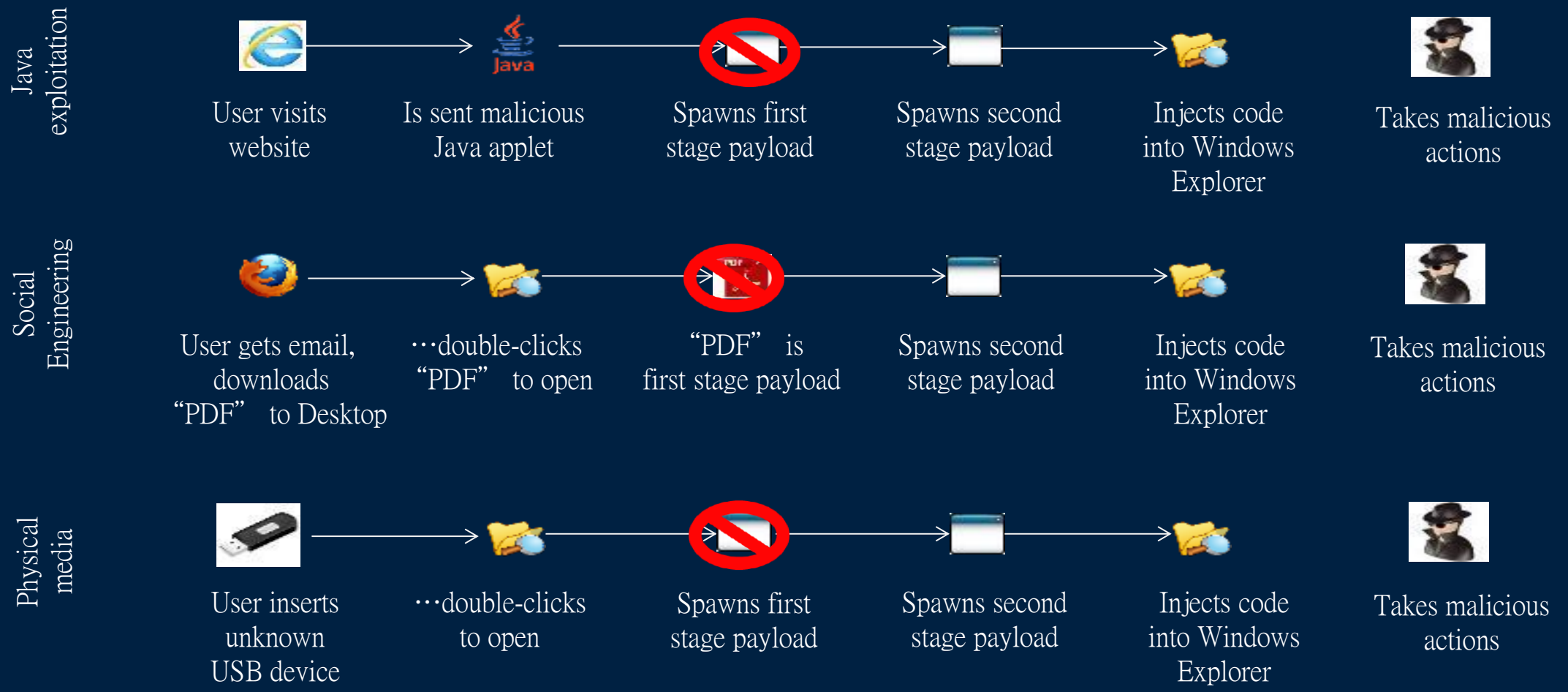
傳統的防毒軟體
僅專注在預防上Only



Carbon Black
Provides Full Security Lifecycle

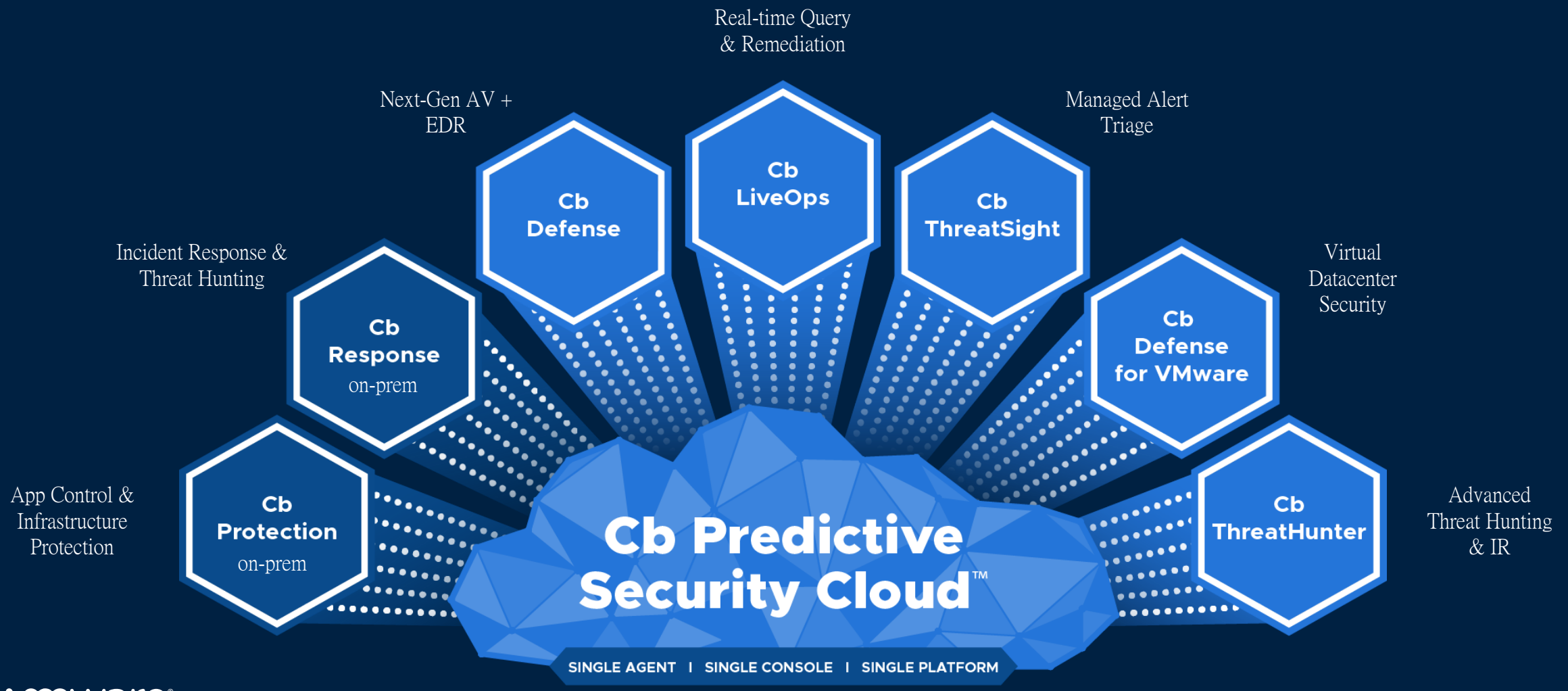


在惡意程式沒發動攻擊前阻斷



vmware Confidential | ©2020 VMware, Inc.

支援雲端版和地端版EDR



Cb Defense 是什麼?

新世代防毒和EDR涵蓋了從防禦到響應的所有範圍

Cb Defense 被認證可取代傳統防毒軟體

Cb Defense 不耗大資源

< 1% of CPU

< 1% of Memory

Cb Defense 防堵惡意軟體含以及malware-less/file-less 攻擊

惡意軟體: known and commodity malware

Malware-less: Living off the land attacks using legitimate tools in OS

PowerShell, python, wmi, javascript, vb script, cmd

Cb Defense提供成熟的EDR以快速進行根本原因分析

Cb Defense提供網路隔離（不使用PowerShell）和Live Response進行補救

Cb Defense 多層次防禦

第1層: 基於簽章的方法：防禦已知和常見的惡意軟件

第2層：來自Carbon Black Predictive Security Cloud的威脅情報

- 來自Cb受保護端點的未過濾數據的協作平台
- 在雲端使用機器學習進行流式分析
- 與Cb以外的多家知名威脅情資供應商整合

第3層：串流防護

- 防禦無惡意軟體/無文件攻擊和記憶體注入
- Powershell，WMI，Python，Ruby，VB腳本，Cmd.exe
- 查看攻擊期間的實際惡意行為

第4層：先進反勒索軟體保護

- 根據已知的攻擊模式檢測並終止零日/未知的勒索軟體
- 由Cb Defense進行金絲雀文件(canary files)誘捕
- 執行刪除備份副本的命令

第5層：提交未知Binaries /.EXE進行分析（基於Cb雲端的沙箱）

- PE檔頭文件：exe，dll
- 壓縮4MB及以下
- 本地簽名包檢測不到任何東西
- CBD PSC雲沒有或信任度低
- 本地ML顯示風險評分（4分及以上）

Cb Defense：主要應用情境

取代傳統防毒之不足

Stop malware & non-malware attacks

- 勒索軟體攻擊防護
- APT攻擊防護
- 無檔案式(fileless)攻擊防護
- 記憶體攻擊防護
- 未知的惡意軟體及零日攻擊(zero-day attacks)防護

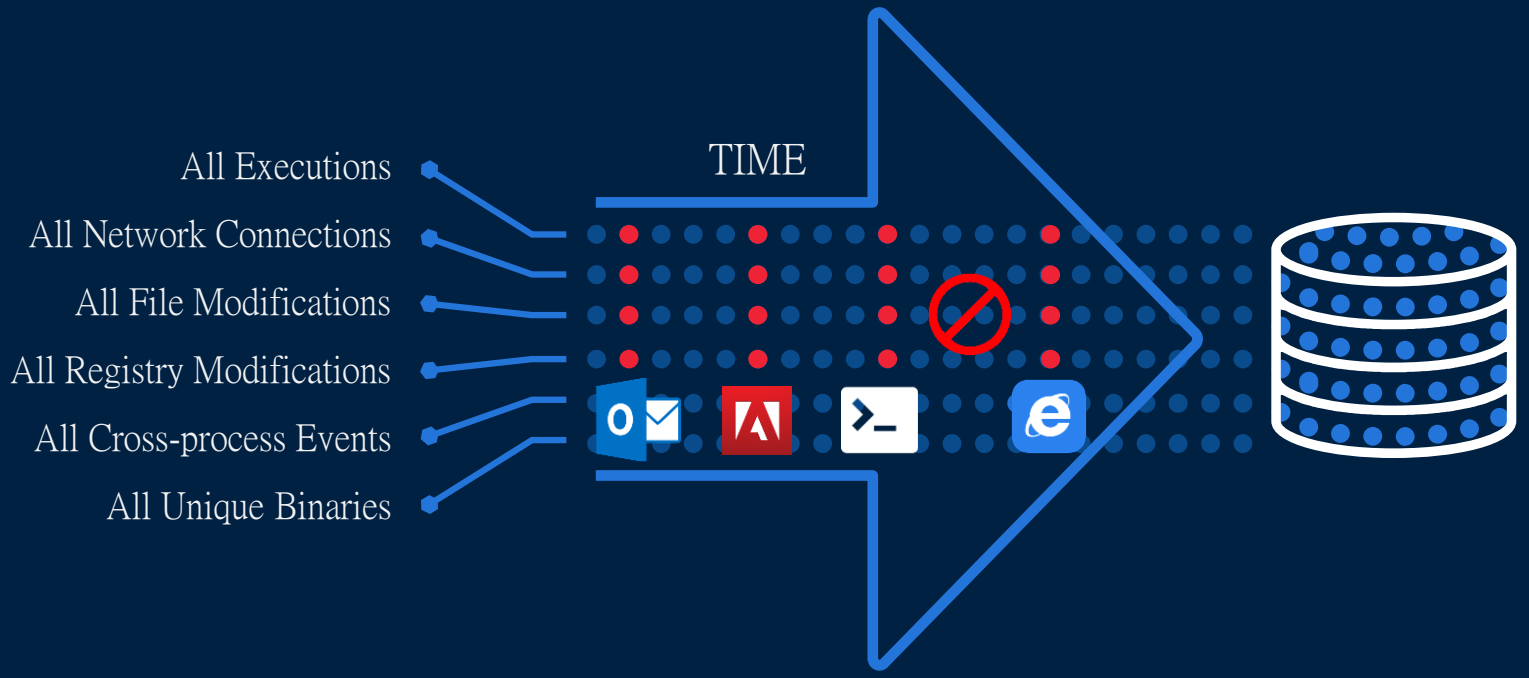
事件偵測回應

Detect and respond to threats in real-time

- 提供事件深度調查機制
- 提供對攻擊的根本原因和機器位置的可視性
- 當已知好的應用程式受到威脅,提供識別及告警之功能
- 具備遠端取證機制,EX:memory dumps

Streaming Analytic即時收集各種訊息

防止已知和未知攻擊



Ransomware bypasses AV and machine learning using trusted software

Assesses risk over time, not just at a single point in time

Prevents and detects known and unknown attacks

Leverages Event Stream Processing – pioneered in fraud detection and algorithmic trading

defense-prod05.conferdeploy.net/?s[version]=1&s[searchWindow]=ONE_WEEK&s[dataGrouping]=NO_GROUP_RESULTS&s[c][SEVERITY][0]=WARNING&s[c][THREA...

Carbon Black.

Notifications 1 | Help | David Hoi (cb-internal-se-dhoi05.com)

CB-INTERNAL-SE-DH...

- DASHBOARD
- ALERTS
- INVESTIGATE
- LIVE QUERY
- ENFORCE
- ENDPOINTS
- SETTINGS

View data: 1 week | All policies

Configure Dashboard | Export All

Attacks Stopped

0

Non-Malware	0
Potential m...	0
Malware	0
PUPs	0

Potentially Suspicious Activity

8

Non-Malware	1
Potential m...	0
Malware	7
PUPs	0

Endpoint Health *

40

Active	7
Inactive	31
Deregistered	2
Eligible for upd...	1
Quarantined	0
Bypass	0

** Current data only; dashboard filters do not apply*

Threat Reports

TAU-TIN - SNAKE Ransomware
5:01:58 pm Jan 23, 2020

TR-4150 - Zeppelin Ransomware
2:04:16 am Jan 23, 2020

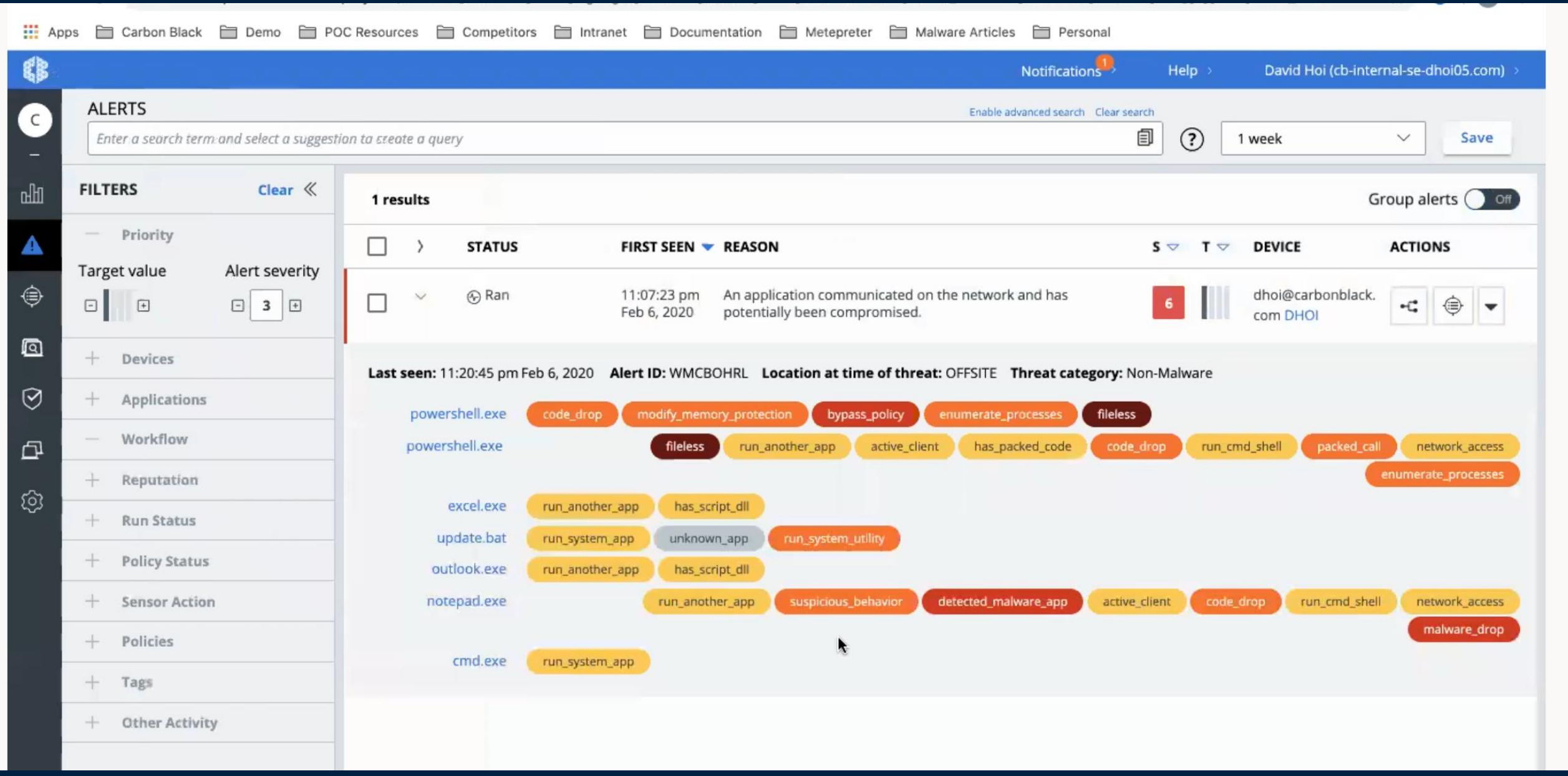
ZeroClear and Dustman Wiper Malware
4:02:03 am Jan 18, 2020

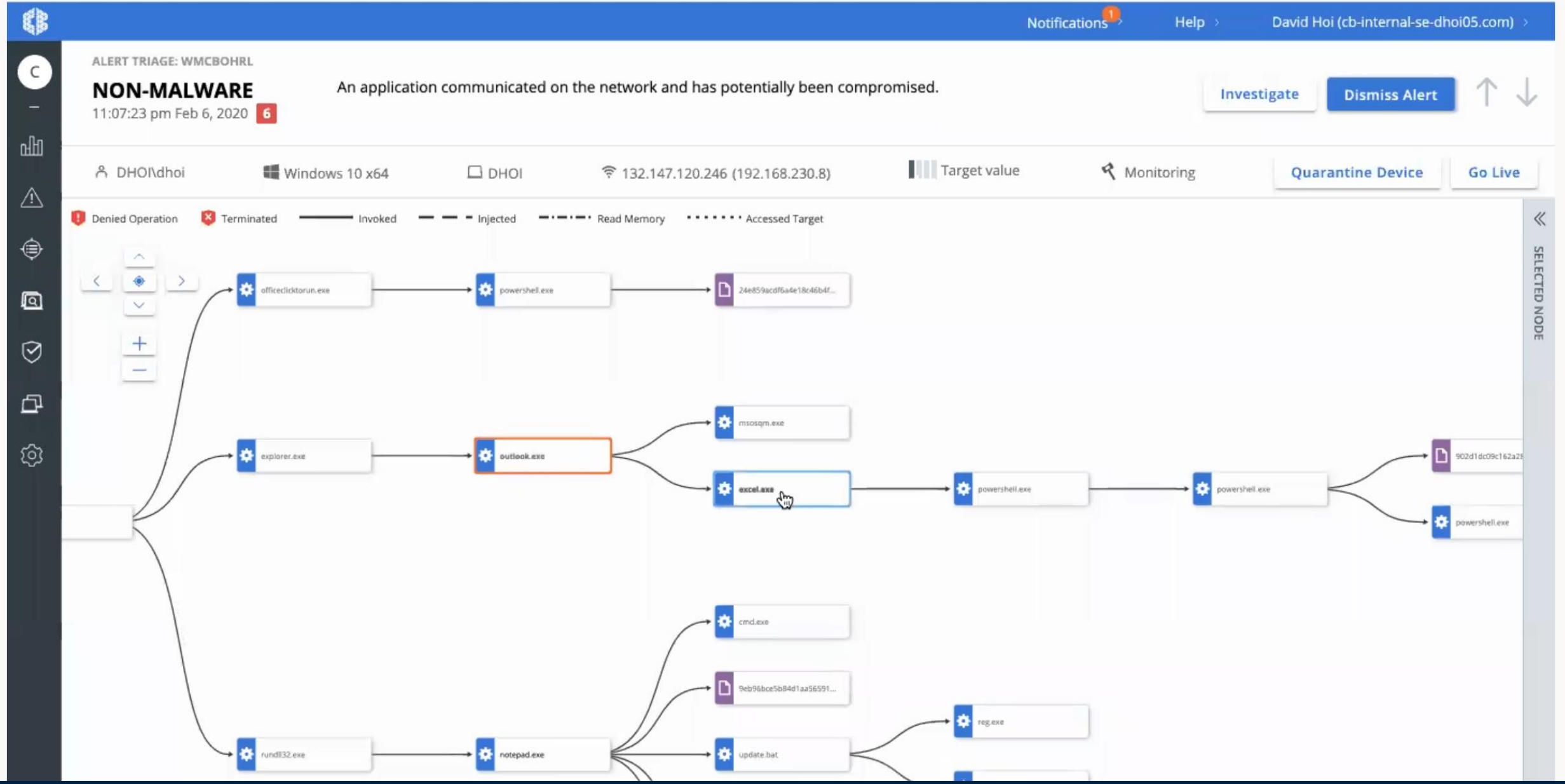
TAU-TIN - SatanCryptor Ransomware

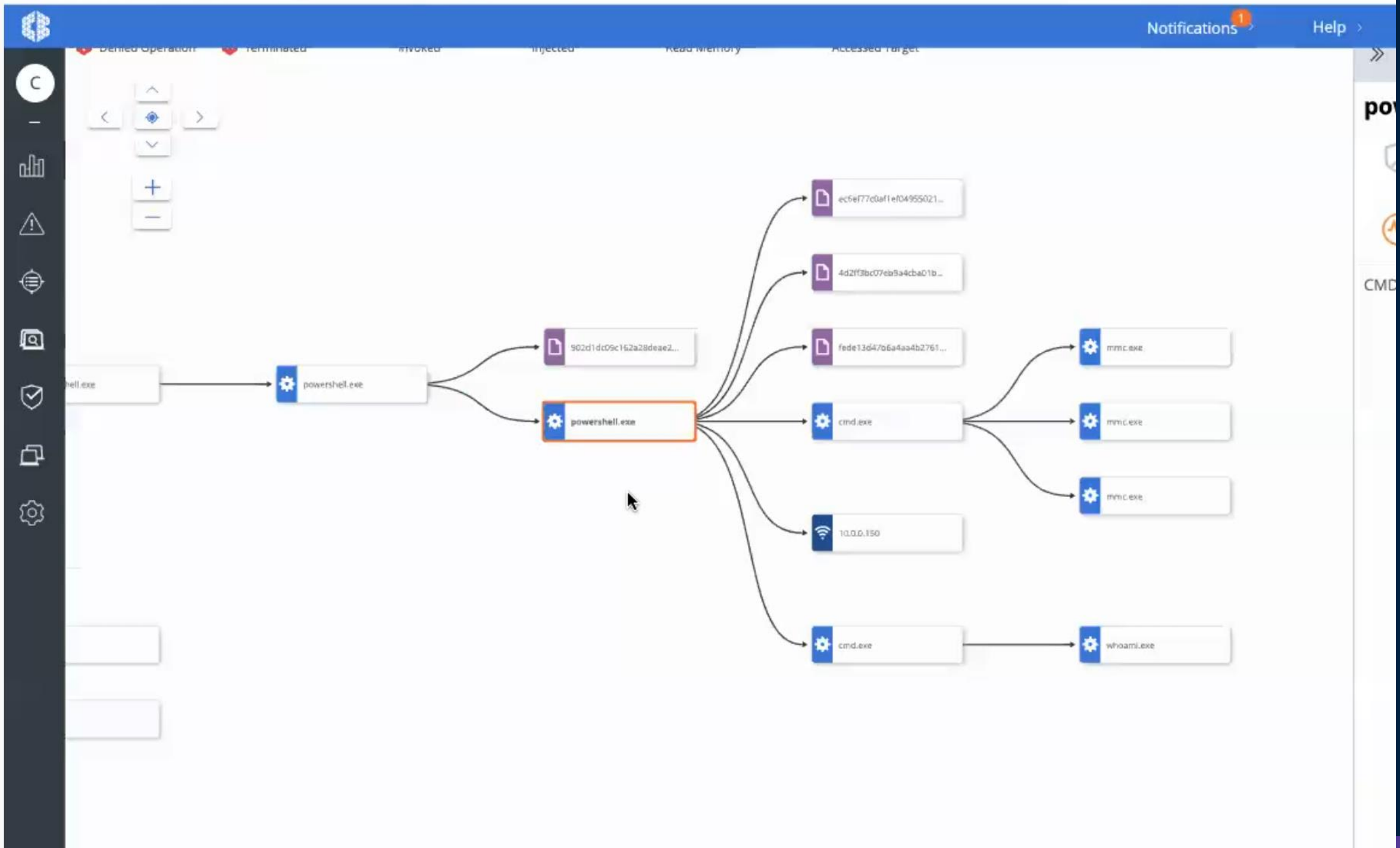
Reports available on the User Exchange

Attacks By Vector

Email	0.0%
Web	0.0%
Remote drive	0.0%
Other net protocol	100.0%
Removable media	0.0%


Apps
Carbon Black
Demo
POC Resources
Competitors
Intranet
Documentation
Metepreter
Malware Articles
Personal
Notifications
Help
David Hoi (cb-internal-se-dhoi05.com)
ALERTS
Enable advanced search
Clear search
Enter a search term and select a suggestion to create a query
1 week
Save
FILTERS
Clear
Priority
Target value
Alert severity
3
Devices
Applications
Workflow
Reputation
Run Status
Policy Status
Sensor Action
Policies
Tags
Other Activity
1 results
Group alerts
Off
STATUS
FIRST SEEN
REASON
S
T
DEVICE
ACTIONS
Ran
11:07:23 pm Feb 6, 2020
An application communicated on the network and has potentially been compromised.
6
dhoi@carbonblack.com DHOI
Last seen: 11:20:45 pm Feb 6, 2020
Alert ID: WMCBOHRL
Location at time of threat: OFFSITE
Threat category: Non-Malware
powershell.exe
code_drop
modify_memory_protection
bypass_policy
enumerate_processes
fileless
powershell.exe
fileless
run_another_app
active_client
has_packed_code
code_drop
run_cmd_shell
packed_call
network_access
enumerate_processes
excel.exe
run_another_app
has_script_dll
update.bat
run_system_app
unknown_app
run_system_utility
outlook.exe
run_another_app
has_script_dll
notepad.exe
run_another_app
suspicious_behavior
detected_malware_app
active_client
code_drop
run_cmd_shell
network_access
malware_drop
cmd.exe
run_system_app


Notifications 1
Help
David Hoi (cb-internal-se-dhoi05.com)
ALERT TRIAGE: WMCBOHRL
NON-MALWARE
11:07:23 pm Feb 6, 2020
6
An application communicated on the network and has potentially been compromised.
Investigate
Dismiss Alert
DHOI\dhoi
Windows 10 x64
DHOI
132.147.120.246 (192.168.230.8)
Target value
Monitoring
Quarantine Device
Go Live
Denied Operation
Terminated
Invoked
Injected
Read Memory
Accessed Target
SELECTED NODE
officeclicktorun.exe
powershell.exe
24e859acdf6a4e18c46b4f...
explorer.exe
outlook.exe
msosqm.exe
excel.exe
powershell.exe
powershell.exe
902d1dc09c162a2...
powershell.exe
cmd.exe
9eb96bce5b84d1aa56591...
reg.exe
rundll32.exe
notepad.exe
update.bat


Notifications
1
Help
Denied Operation
Terminated
Invoked
Injected
Read Memory
Accessed Target
hell.exe
powershell.exe
902d1dc09c162a28deae2...
powershell.exe
ec6ef77c0af1ef04955021...
4d2ff3bc07eba9a4cba01b...
fede13d47b6a4aa4b2761...
cmd.exe
10.0.0.150
cmd.exe
mmc.exe
mmc.exe
mmc.exe
whoami.exe
CMD

Cb Protection-先進端點應用程式智能防護

軟體白名單+行為黑名單雙重防護

CB PROTECTION

APP CONTROL

on-prem

威脅預防

- 應用程式控制
- 阻擋惡意程式(含Script)及進階持續性威脅(APT)
- 防止所有惡意或未經授權的變更
- 裝置控制

符合法規

- 保持對關鍵框架的持續合規性，包括PCI-DSS，HIPAA，GDPR，SOX，FISMA和NERC
- 監視關鍵活動並執行配置，評估風險並維護系統完整性
- 通過強大的變更控制和白名單策略保護報廢系統

智能管理

- 提供豐富且靈活的隨套即用範本
- 多種自動化批准策略
- 輕量及高效能的代理程式
- 自動分析並阻止系統上所有新增高風險的文件

Cb Protection：主要應用情境

PLATFORMS • Sensor Support: • Windows XP, Server,Vista, Embedded, POS • Mac OS X • RHEL Linux • CentOS Linux • Oracle RHCK Linux

固定功能設備

POS 收銀機系統, ATM 提款機, 加油幫浦

- Vulnerable & exposed
- Data is valuable
- Downtime is expensive

資料中心主機

機房主機Servers, 網域主控站 & VDI 虛擬桌面

- Most targeted asset
- 99.99% uptime required
- Agent fatigue

工業控制系統

關鍵基礎建設自動控制設備

- Massive exposure
- More devices & automation
- Increasingly connected
- Increasingly regulated

受控制的端點

高階主管/客服中心/ Kiosks 站台

- Call Centers
- Executive PCs
- Financial systems
- Healthcare systems

Cb Response-端點威脅態勢感知系統

偵測分析及回應各種先進威脅

CB RESPONSE
SOC & IR
on-prem

全面透視

- 捕獲所有活動
- 透視攻擊鏈
- 識別根本原因，找出入侵根源
- 事件集中儲存與回朔調查

攻擊預測

- 將各式威脅情資進行大數據分析
- 快速找出潛在未知威脅
- 多種潛在未知威脅偵測技術
- 先進的威脅預測分析
- 整合式防護，強化縱深防禦

即時的回應機制

- 隔離受駭端點，避免威脅擴散
- 遠端蒐集數據，鑑識分析
- 修護遭感染端點，防止再次受駭
- 一鍵阻擋，防護所有端點
- 受駭範圍一目了然

vmware® Confidential | ©2020 VMware, Inc.

Cb Response：主要應用情境

強化SOC

市佔率最高的 EDR
端點偵測/事件因應

- 填補端點的防護盲點
- 達到更快的回應時間
- 解決疲乏的大量事件
- 找出事件發生根本原因
- 找出防毒偵測不到的惡意程式

威脅獵捕

以先進的戰術
打擊駭客

- 避免先進攻擊躲過既有防護
- 希望找出攻擊的手法
- 萃取出攻擊手法的威脅情資
- 獵捕環境內潛在未知威脅

獲 IBM 安全團隊, 中華資安,數聯資安, 關貿引用

變成企業資安
的基礎

- 太多的漏洞
- 修補疲於奔命
- 缺乏威脅的可視度
- 缺乏資安人力與預算

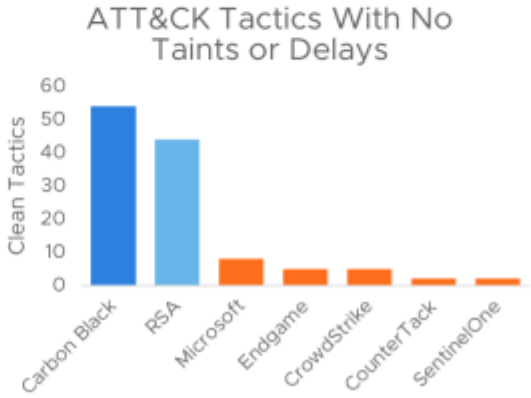
MITRE ATT&CK™ EVALUATION RESULTS: APT3

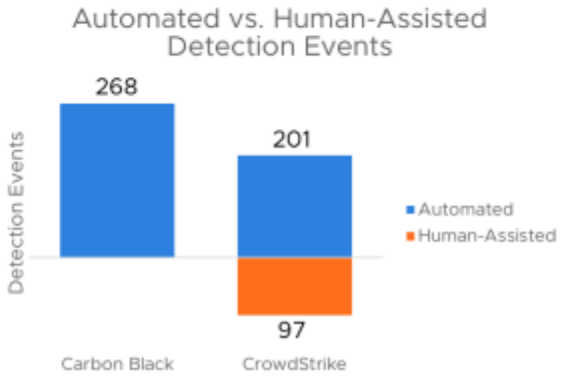
Carbon Black Outperforms All Other EDR Solutions

MITRE's public evaluation of endpoint detection and response (EDR) products demonstrated why Carbon Black is a top choice of security and IT professionals and showcased how Carbon Black detects sophisticated attacks quickly, so teams can respond confidently.

This test was based on MITRE's popular ATT&CK™ framework and represents a new approach to EDR testing: open, sophisticated, rigorous, and reflective of the real world. In the first test, which mirrored the tactics, techniques and procedures of APT3, Carbon Black demonstrated strong results that set us apart from the rest of the security products tested. Carbon Black showed:

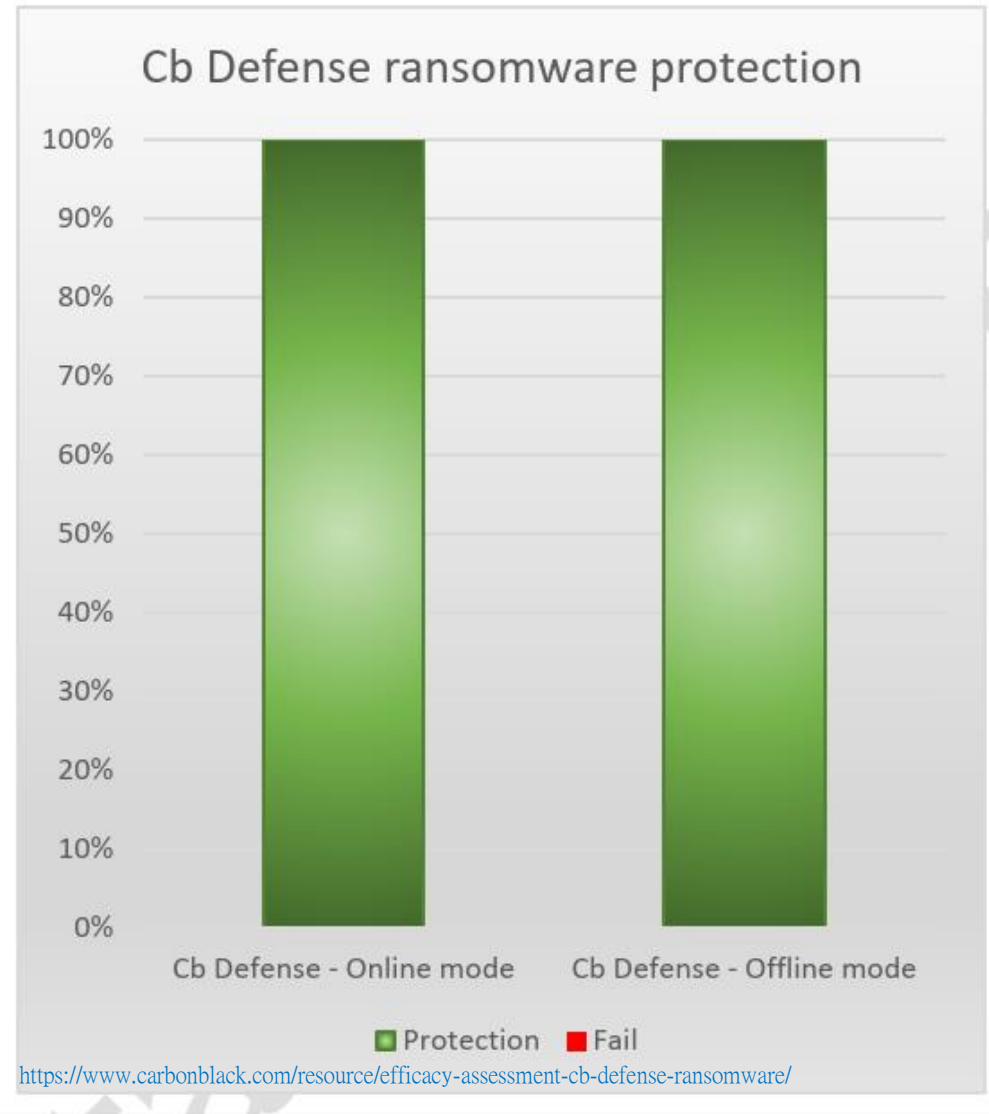
- **Speed:** Zero delayed detections, so you can respond faster before the attack gets worse
- **Confidence:** Zero tainted detections, so you know that threats will be detected even as attackers change tactics
- **Predictability:** Zero reliance on humans in the loop, so you know detections will not be dependent on human intervention





MITRE 對基於ATT&CK知識庫的端點檢測及響應（EDR）產品的評估，不僅能夠評估這套知識庫的服務與效果，還將確定基於ATT&CK的EDR產品是否具備檢測高級威脅的能力。。

勒索軟體100%防禦



- 使用高達42種不同家族的勒索軟體進行測試
  - WannaCry, Locky,Petya, NotPetya and Petya Goldeneye…etc
  - MBR/MFT/boot record
  - File-less ransomware
  - EXE, DLL, script based ransomware
  - Unique samples dropped by exploit kits
  - Ransomware targeting the Volume Shadow Copy (deleting it via vssadmin)

Cb Cloud 每天收集1.3兆Events

A Cloud-based Platform that Marries Threat, Infrastructure and Application Context

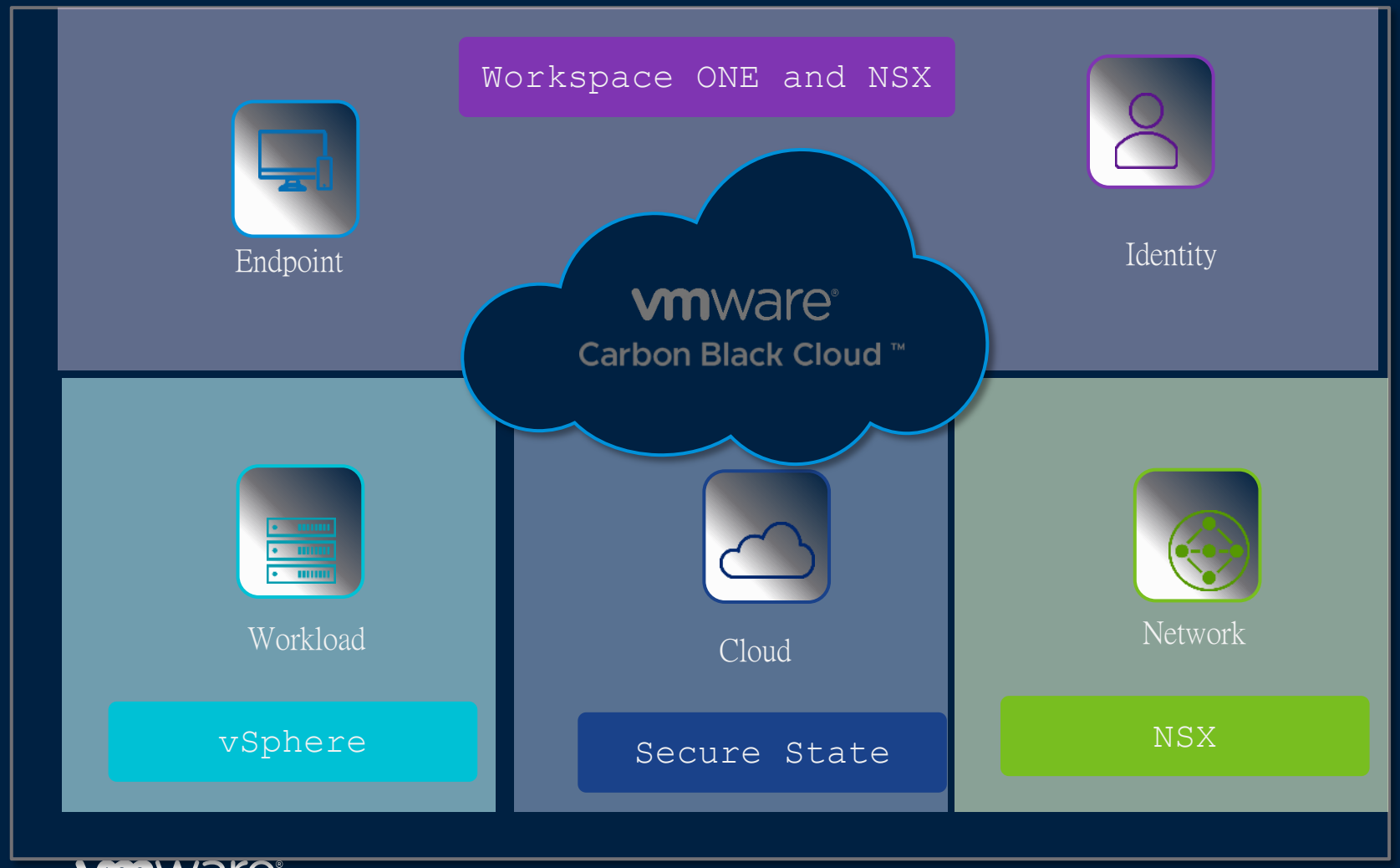
Platform

ML/Big Data Analytics

Monitor millions of endpoints and workloads, analyzing over 540TB of endpoint data and over 1.3 trillion events per day*

Carbon Black會整進VMware 其他Solutions

Enabling Better Context, Control, and Collaboration



學習

透過CB 學習Application狀態

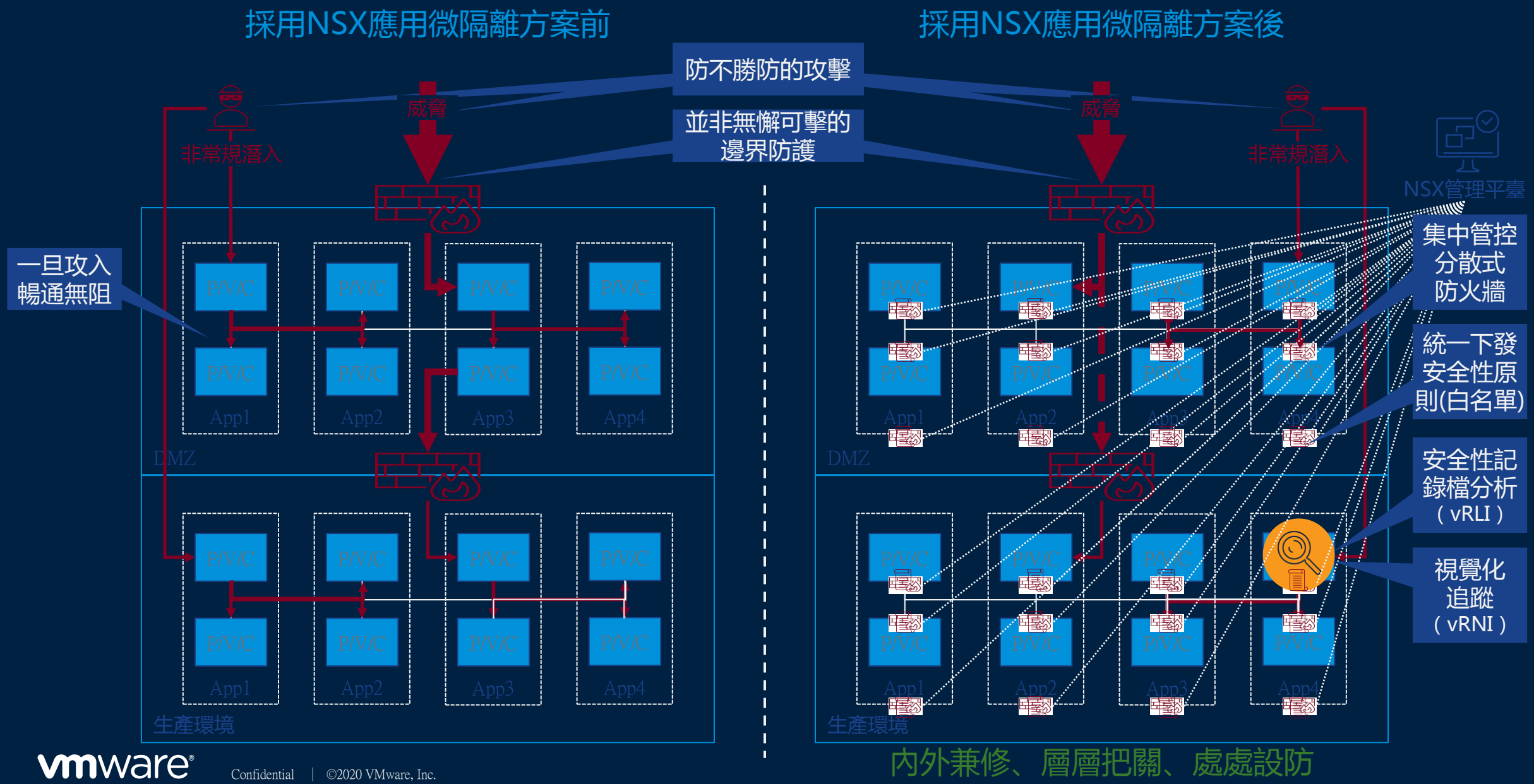
保護

NSX保護前門, CB保護後門, VRNI整合CB Cloud

調適

CB trigger NSX 防火牆規則

採用VMware NSX讓實體機, 虛擬機和Container都自帶Firewall



vmware
Confidential | ©2020 VMware, Inc.

可以整合的各種方案夥伴

Cloud
- netskope

Endpoint
- Microsoft

Vulnerability & Configuration
- BIGFIX

Training
- wombat security technologies

SIEM
- Radar
- splunk>
- LogRhythm

Analytics
- CLICK SECURITY
- exabeam
- niara
- VECTRA

Automation & Orchestration
- DEMISTO
- Phantom
- sqrrl

Threat Intelligence
- Microsoft

Network & Perimeter
- BLUE COAT
- Check Point SOFTWARE TECHNOLOGIES LTD.
- CYPHORT
- DAMBALLA
- Fidelis Cybersecurity
- FORTINET
- Infoblox CONTROL YOUR NETWORK
- lastline

產品受領先的分析公司和出版物認可

Gartner peerinsights™

MOST 5-STAR RATINGS

A Gartner Peer Insights
Customers' Choice for EDR Solutions
January 2019

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2019

BEST PRODUCT ENDPOINT SECURITY

Cyber Defense Magazine
2019 InfoSec Awards

MITRE ATT&CK™

LEADER IN DETECTING THREATS

MITRE ATT&CK Evaluation
November 2018

Gartner®

A VISIONARY

Gartner Magic Quadrant for
Endpoint Protection Platforms
2019

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2019

BEST CYBERSECURITY COMPANY & BEST ENDPOINT SECURITY SOLUTION

2019 Cybersecurity Excellence Awards

FORRESTER®

STRONG PERFORMER

The Forrester Wave™
Endpoint Security Suites
2019

總結

- 完美整合VMware其他產品
- 針對未知攻擊EDR領導廠商
- 支援雲端版和不上雲端版
- 支援多樣平台single agent 五Layer防禦
- 透過大數據可把傳統signatures 歸類到100種攻擊行為, 加快偵測速度
- 可以分析出攻擊路徑並進行攔阻

Thank You

Please email any questions to PowerPoint@vmware.com

vmware®

Confidential | ©2020 VMware, Inc.