

TM

Fidelis Elevate解決方案

端點Endpoint

Agenda

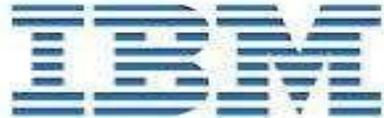
- Fidelis公司簡介
 - 閘道Network
 - 端點Endpoint
 - 誘捕Deception
 - 聯防防禦架構
-

Why Fidelis

- Gartner : APT防禦架構5大技術，企業至少要具備兩項以上
 - 網路流量分析
 - 網路鑑識
 - Payload分析
 - 端點行為分析
 - 端點鑑識
 - Fidelis 全部具備
-

Fidelis公司簡介

Fidelis深受世界上最重要品牌的信賴



- Apple 100G流量
 - 微軟全球每個分點都有Fidelis
 - 美國海軍DLP、空軍每年合約超過23.6million
 - Barclays(巴克萊銀行)12萬個Endpoint
 - IBM mail solution
 - 美國Samsung mysingle protocol
-

Fidelis 多項資安認證與得獎紀錄

唯一獲得通用標準(CC)安全認證

通過美國 Sandia 國家實驗室的紅隊(Red team)測試

符合美國聯邦政府單位網路的加密要求FIPS 140-2加密驗證

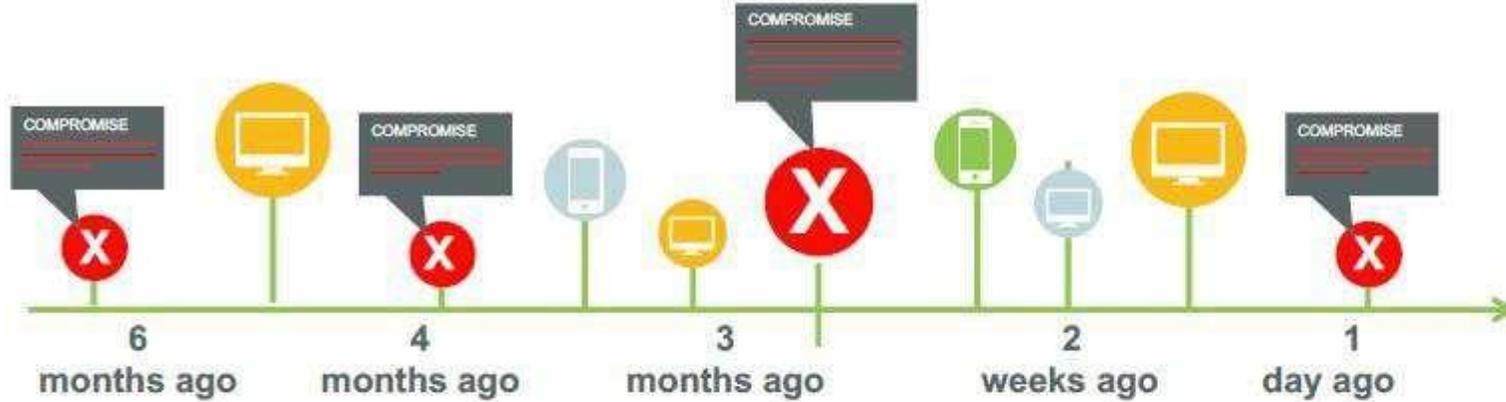
獲得GCN實驗室評論選擇獎

美國軍隊資訊安全保障名錄唯一建議採購的資安產品



Fidelis 在每個時間點都可以查到攻擊事件

- 除了即時檢測外，Fidelis還可以让您看到在先前發生的攻擊



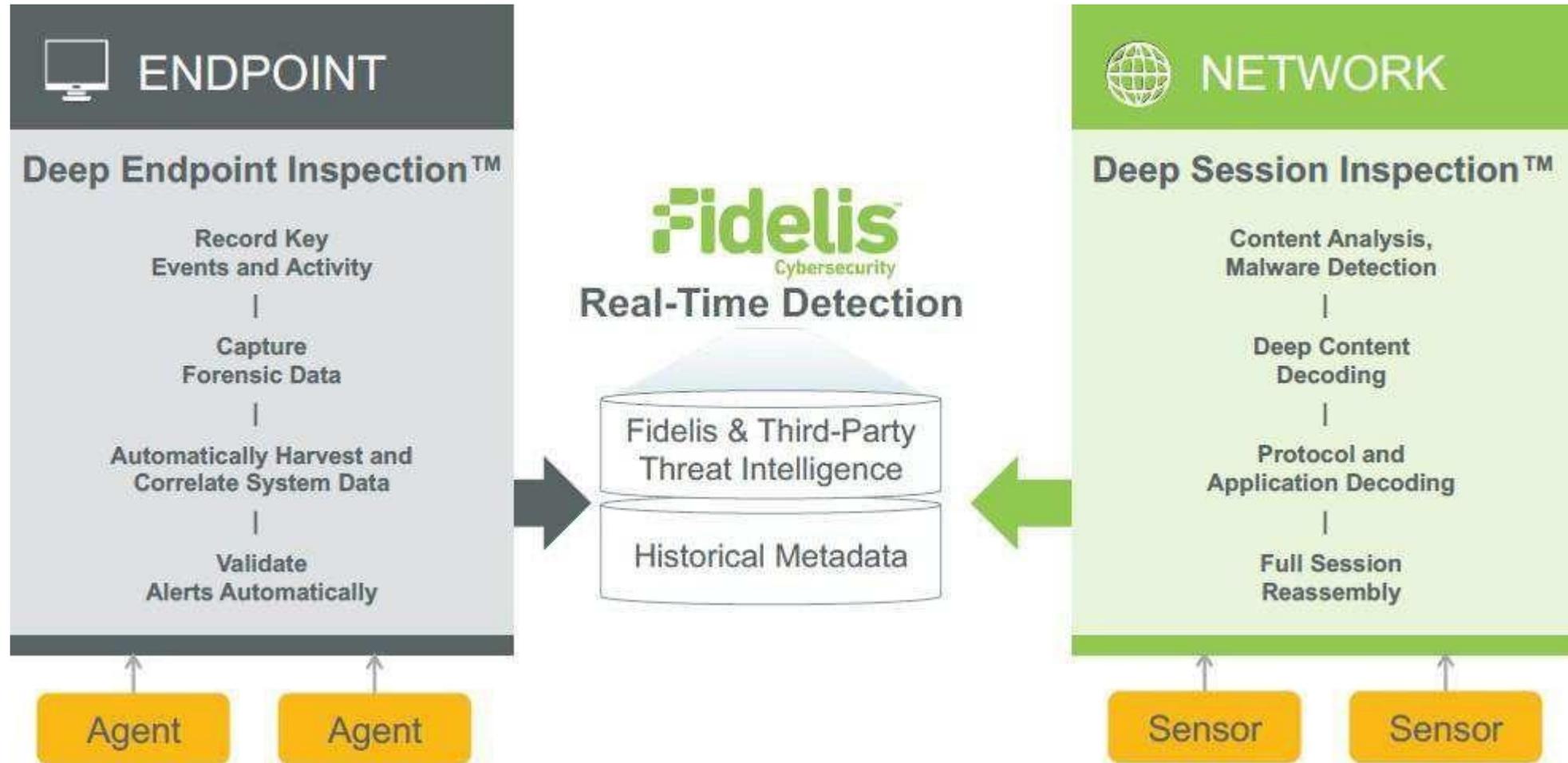
歷史資料

用情資比對歷史資料
調查告警及發生事件
偵測多維度攻擊
使用歷史資料獵殺攻擊者
看看網路上發生什麼

TODAY

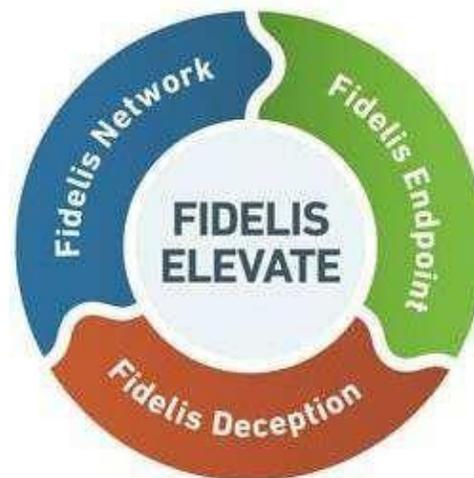
確認告警
識別攻擊者活動
比對第三方威脅情資
阻擋資料外洩

Fidelis 如何偵測攻擊



Fidelis Elevate

- 整合多個解決方案：
 - Network：網路流量監控、資料外洩防護、網路鑑識(NDR+DLP+NF)
 - Endpoint：端點防護、事件反應及端點鑑識(XDR+EF)
 - Deception：駭客誘捕科技
- 自動化的威脅偵測、獵捕和事件反應平台自
- 動驗證、關聯和事件反應
- 快速地偵測、強化獵捕駭客
- 調查歷史軌跡和瞭解事件來龍去脈



Fidelis Network®

全端口協定分析
全面網路可視性
威脅偵測與反應
防範機敏資料洩漏



Fidelis Endpoint®

端點防護與管理
整合單一 Agent
自動化偵測與反應
完整事件鑑識調查

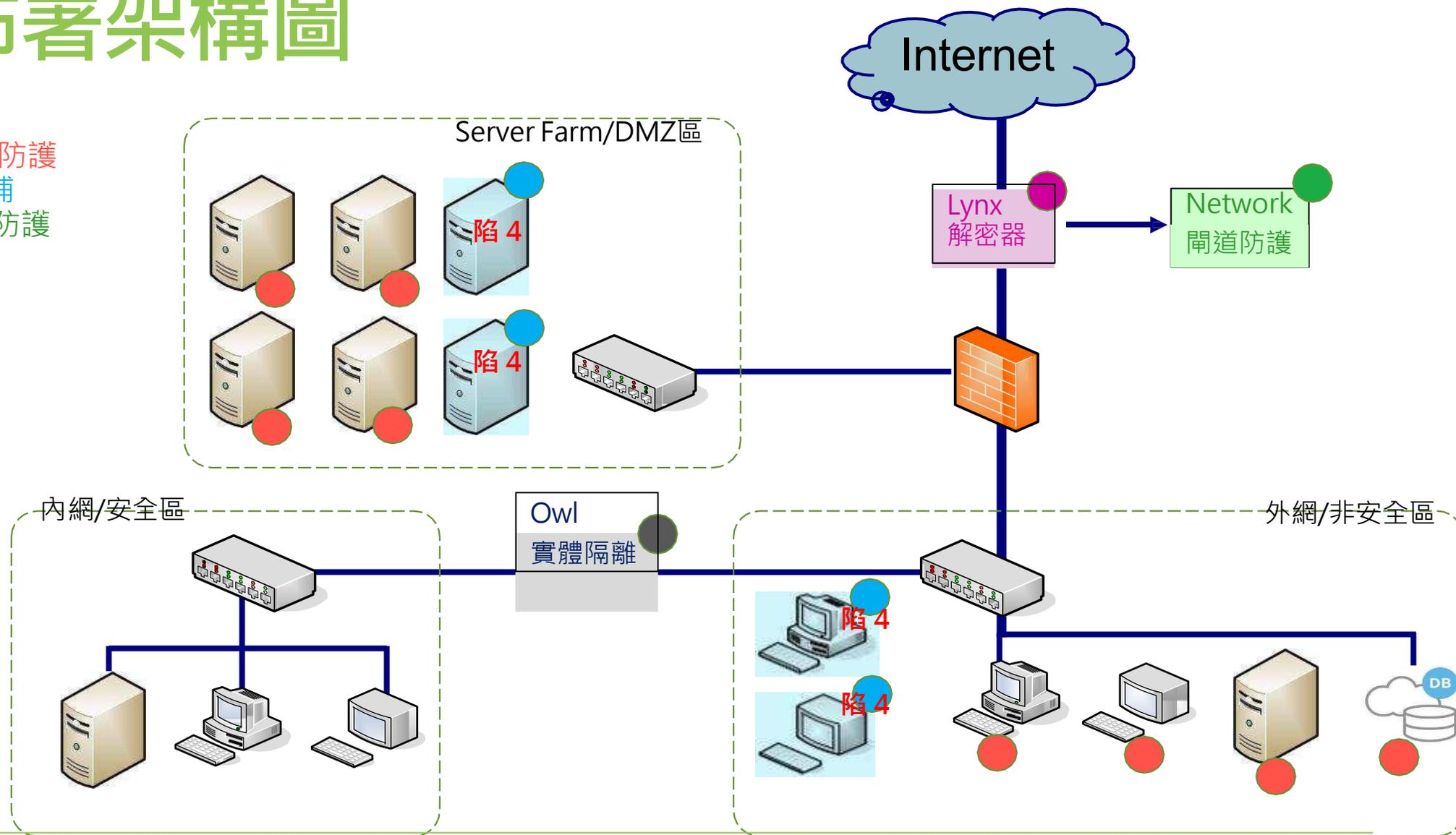


Fidelis Deception®

駭客誘捕技術
企業資產盤點
自適網路環境變化
全自動化誘餌佈署

實際佈署架構圖

- Endpoint端點防護
- Deception誘捕
- Network閘道防護
- Lynx解密器
- Owl實體隔離



端點Endpoint

Endpoint 端點防禦功能

記錄/監控

- 端點事件全部紀錄
- 行為規則偵測
- 內建防毒軟體
- 端點設備狀態管理

調查分析

- 圖像化執行緒分析
- 內建調查鑑識工具
- 禱現未知威脅的行為告警規則

處理

- 遠端收集資料檔案或上傳更新
- 端點網路隔離
- 執行矯正程序
- Network、Endpoint 聯防

內建偵測規則即時監控未知攻擊

Enable the automatic import of detection rules from Fidelis.

Search [] [] []

<input type="checkbox"/> []	Name	Severity
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Behavior: T1566.001 - Microsoft Word Loading WMI DLLs	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Registry: T1547.005 - Security Support Provider Modified	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Process: Emotet PowerShell execution	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Behavior: T1505.003 - Server Software Component - IIS Web Shell	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Registry: T1548.002 - Bypass UAC - High Integrity Process Registry Keys	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Process: T1047 - WMIC remote process execution	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Process: T1021.001 - RDP Redirect Hijack Detected	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Process: MITRE ATTACK - System Utility Invoked by Office Product	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Process: T1562.001 - Disable Syslog (Linux)	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Behavior: T1547.004 - Boot or Logon Autostart Execution: Winlogon Helper DLL	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Behavior: PowerShell Invoked Web Request to Public IP Address	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	File: Fake System File Created	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Registry: T1137.002 - Office Special Key Modified	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Process: T1027 - PowerShell passed Base64 encoded string and hidden command-line ...	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	File: T1201 - BloodHound Zip File Written	High
<input type="checkbox"/> [] <input checked="" type="checkbox"/>	Registry: T1546.008 - Accessibility Features Hooked via Registry - Potential Backdoor	High

Showing 101 to 200 of 646 items

- Detection Rule內建超過600類型的規則，即時在端點進行偵測與保護
- 偵測MITRE攻擊行為類型、CVE弱點和Microsoft KB
- 針對多種駭客攻擊手法進行檢測
 - Powershell無檔案攻擊
 - Phishing等傳統滲透手法
 - 系統防火牆/目錄/檔案/機碼等異常行為
 - 已知APT攻擊手法
- 可測試未知勒索軟體行為並阻擋執行

加入多種情資與特徵碼偵測

Configuration / Threat Intelligence / Intelligence Feeds 2021/10/04 07:41 UTC | administrator |

Search [] [] [] + Add Feed + Add Fidelis Feeds []

<input type="checkbox"/>	Name	Total Indicators	Last Updated
<input type="checkbox"/>	Allow list	0	2021/10/04 01:22:12
<input type="checkbox"/>	Block List	0	2021/07/14 06:55:44
<input type="checkbox"/>	Fidelis Intelligence - Malicious Files	1577630	2021/10/04 05:57:10
<input type="checkbox"/>	Fidelis Intelligence - Suspicious Files	339192	2021/10/04 05:53:22
<input type="checkbox"/>	Fidelis Intelligence - Suspicious Network	6944	2021/10/04 05:57:10
<input type="checkbox"/>	Sandbox - malicious executables	0	2021/10/04 01:22:12

Showing 1 to 6 of 6 items

- 定期自動更新
- 包含確認Malware的資料庫
- 可疑檔案的資料庫
- 黑名單URL
- 沙箱驗證判定為惡意的可執行物件

內建防毒軟體偵測已知病毒/APT

The screenshot displays the configuration interface for the 'All' group in the Fidelis Elevate console. The 'AntiVirus' tab is selected, and the 'Global AntiVirus Settings' section is visible. The 'Enable AntiVirus' toggle is turned on, and the text 'POWERED BY Bitdefender' is displayed to the right. Below this, there are options for 'Enable Advanced Malware Detection' and 'Improve AntiVirus Performance by Communicating with Cloud Services'. There are also sections for 'Exclusion Directories' and 'Exclusion Extensions', each with an 'Add a field...' input. A 'Save' button is located at the bottom right of the settings panel.

Configuration / Groups

Groups

Search

Group: All

Endpoints AntiVirus Process Scanning Event Monitoring

Global AntiVirus Settings

Enable AntiVirus POWERED BY Bitdefender

This will enable AntiVirus for all computers. Group settings will override this default.

Enable Advanced Malware Detection

Improve AntiVirus Performance by Communicating with Cloud Services

Exclusion Directories:

Add a field...

Exclusion Extensions:

Add a field...

Save

知名品牌
BitDefender

- APT+防毒
- 偵測已知惡意程式

告警自動匯整本次攻擊所有事件

The screenshot displays the 'Investigation / Behavior Details' window for the process 'msixec.exe' on 'LAPTOP-10UNBUD9'. The process summary shows it was started at 2023/06/28 01:19:21.341 and ended at 01:19:22.262. A 'Process Start' timeline shows the process beginning at 20s. A 'File Write' event is highlighted, showing the file 'QualityUpdateAssistant.dll' was written to 'C:\Windows\System32\QualityUpdateAssistant.dll' at 01:19:21.959 by 'NT AUTHORITY\SYSTEM'. Below the timeline, a table lists file operations:

Alerts	Parent	Process Tree	All Behaviors	Remote Threads	Executables/Libraries	File	Registry	Threat Lookup 0
1						File Write		
						File Create		
1						File Write		
						File Create		

The 'File Target' pane shows details for the file write event: Action: msixec.exe wrote to this file., Behavior: File Write, Name: QualityUpdateAssistant.dll, Path: C:\Windows\System32\QualityUpdateAssistant.dll.

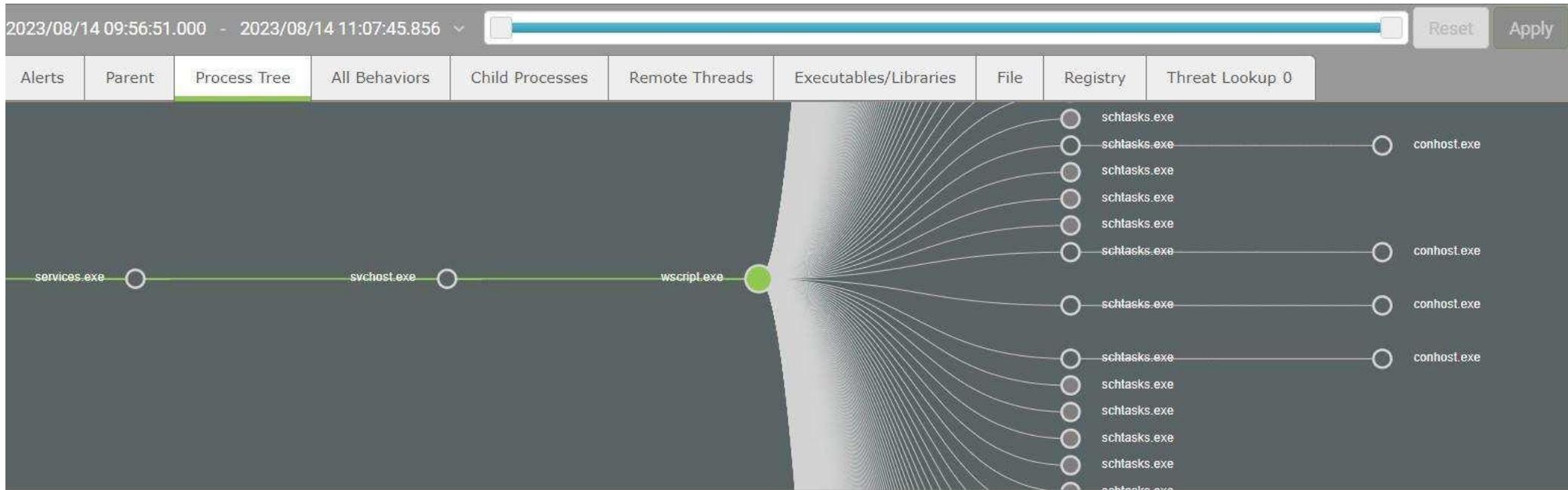
- 每個告警均自動繪出程序流程圖
- 自動收集各類型細節
 - 父程序與子程序 行為動作
 - 遠端連線
 - 使用到的檔案、機碼
- 自動至第三方檢查雲端分數

所有的動作紀錄在All Behaviors內

Alerts	Parent	Process Tree	All Behaviors	Child Processes	Remote Threads	Executables/Libraries	File	Registry	Threat Lookup 0
Time	Type	Summary	Enrichments						
2023/08/14 09:56:51.569	Load Executable/Library	Name msado15.dll Signature Signed Path C:\Program Files\Common Files\System\ado\msado15.dll							
2023/08/14 09:56:51.553	Thread Created by Other	Other Process System Thread ID 14180 Remote PID 4 Module Function							
2023/08/14 09:56:51.553	Registry Create	Hive HKEY_USERS\S-1-5-21-205879... Name Key \Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Softwe							
2023/08/14 09:56:51.522	Registry Create	Hive HKEY_USERS\S-1-5-21-205879... Name Key \Software\Microsoft\Windows Script Host\Settings							
2023/08/14 09:56:51.522	Registry Create	Hive HKEY_LOCAL_MACHINE Name Key \SOFTWARE\Microsoft\Windows Script Host\Settings							
2023/08/14 09:56:51.507	Thread Created by Other	Other Process svchost.exe Thread ID 12028 Remote PID 836 Module Function							
2023/08/14 09:56:51.507	Process Start	Name wscript.exe User WWW\Administrator PID 13868 Signature Signed Command-line C:\Windows\System32\WScript.exe "C:"							

- 在All Behaviors的頁面中，依時間順序紀錄所有的惡意行為
- 被額外呼叫的程序也會進行合法憑證的檢查
- 事件紀錄的時間單位到1/1000秒，可精確分辨出每個動作的先後順序

圖像化執行緒分析



- 告警觸發的執行緒，會將該執行緒的父程序及子程序以樹狀圖表示
- 方便追蹤來源

管理所有端點安裝的軟體

Investigation / Installed Software 2023/11

Search [] [] []

Name	Publisher	Version	Highest CVE Score	CVE Count
Microsoft .NET Framework 4.8	Microsoft Corporation	4.8.03761	8.8 - High	2
Google Chrome	Google LLC	109.0.5414.120	8.8 - High	13
Google Chrome	Google LLC	109.0.5414.168	8.8 - High	13
Google Chrome	Google LLC	118.0.5993.118		0
Google Chrome	Google LLC	119.0.6045.160		0
Chrome 遠端桌面	Google\Chrome	1.0		0
Gmail	Google\Chrome	1.0		0
Google 雲端硬碟	Google\Chrome	1.0		0
YouTube	Google\Chrome	1.0		0
文件	Google\Chrome	1.0		0
簡報	Google\Chrome	1.0		0
試算表	Google\Chrome	1.0		0
Google Earth Pro	Google	7.3.6.9345		0
HPSSupply	Hewlett Packard Develop...	2.1.1.0000		0
64 Bit HP CIO Components Install...	HP Inc.	22.2.1		0
Lotus Notes 8.5.3 (Basic) zh_TW	IBM	8.53.11287		0
Lotus Notes 8.5.3 zh_TW	IBM	8.53.11286		0
7-Zip 22.01 (x64)	Igor Pavlov	22.01		0
7-Zip 9.20 (x64 edition)	Igor Pavlov	9.20.00.0		0
Intel® Graphics Command Center	INTEL CORP	1.100.5237.0		0

Endpoints CVE

Endpoint Name [] [] []

- 自動收集端點上所有安裝的軟體
- 比對版本並檢查是否有CVE漏洞
- 以風險值分數來區分重要性
- 匯整相關端點數量
- 可在主控台直接uninstall端點的安裝軟體

可直接端點操作

The screenshot displays the Endpoint Manager interface. On the left, a list of endpoints is shown, with 'ftp215' selected. The main area shows a file explorer view for the 'FTP' directory on the endpoint. A table lists the files and folders in the current directory.

Name	Size	Owner	Permissions
ArmorX		BUILTIN\Administrators	drwxrwxrwx
Backup		BUILTIN\Administrators	drwxrwxrwx
CentOS for sftp		BUILTIN\Administrators	drwxrwxrwx
Fidelis Endpoint		BUILTIN\Administrators	drwxrwxrwx
Fidelis Network		BUILTIN\Administrators	drwxrwxrwx
FJUArmorXMeeting		BUILTIN\Administrators	drwxrwxrwx
Fudo		BUILTIN\Administrators	drwxrwxrwx
Lynx		BUILTIN\Administrators	drwxrwxrwx
Office 2010		BUILTIN\Administrators	drwxrwxrwx
Others		FTP215\Admin	drwxrwxrwx
Owl		BUILTIN\Administrators	drwxrwxrwx
ReaQta		BUILTIN\Administrators	drwxrwxrwx
ReaQta cloud temp		FTP215\Admin	drwxrwxrwx
RHEL7.9 ISO		BUILTIN\Administrators	drwxrwxrwx
TrendMicroXDR		BUILTIN\Administrators	drwxrwxrwx
ubuntu-18.04.1 ISO		BUILTIN\Administrators	drwxrwxrwx
Windows ISO		BUILTIN\Administrators	drwxrwxrwx
Eventlog.Txt	3.41KB	BUILTIN\Administrators	-r--r--r--
Fidelis Endpoint Services - Ubunt...	9.09KB	FTP215\Admin	-r--r--r--

- 只要端點是上線狀態，就可以從主控台進行端點直接操作
- 可進行的操作有：
 - 檔案上傳/下載
 - 複製/剪下/貼上
 - 刪除/移動
- 可直接開啟命令列 (Windows Command Line)

系統管理功能可執行更複雜的作業

- 取回指定檔案
 - 搜尋特定檔案
 - 清除指定檔案
 - 目前執行中程序列表
 - 清除指定程序
 - 防毒軟體狀態端
 - 端點防火牆規則
 - 端點所有帳號
 - 目前網路連線
 - 目前service狀態
 - 還原Windows restore point
 - CPU loading
 - 硬體資訊
 - USB drive狀態
 - 登入成功/失敗紀錄
 - 瀏覽器歷史紀錄
 - 無線網路連線紀錄
 - 記憶體分析
 - 搜尋指定機碼
 - CVE弱點報告
 - IOC掃瞄
 -
-

鑑識工具

The screenshot displays a web-based interface for investigating behaviors. The top navigation bar shows 'Investigation / Behaviors' and the current time '2023/07/18 09:42 UTC'. A user dropdown menu is set to 'administrator'. A sidebar on the left lists various system categories, with 'USB' selected. The main area features a search bar and a date range filter for 'June 18, 2023 09:42:39 - July 18, 2023 09:42:39'. Below this is a table with the following columns: Endpoint, Drive Letter, Serial, Model, Media, and Type. The table contains several rows of data, including events for 'LAPTOP-10UNBUD9' involving 'Kingston DataTraveler 3.0' and 'Generic Mass Storage' devices.

Endpoint	Drive Letter	Serial	Model	Media	Type
LAPTOP-10UNBUD9	E:	4CEDFB74A543F4B0B96B0137	Kingston DataTraveler 3.0	USB	USB Attach Device
LAPTOP-10UNBUD9	E:	80ABEE5E	Generic Mass Storage	USB	USB Remove Device
LAPTOP-10UNBUD9	E:	80ABEE5E	Generic Mass Storage	USB	USB Attach Device
LAPTOP-10UNBUD9	E:	80ABEE5E	Generic	USB	USB Remove Device
LAPTOP-10UNBUD9	E:	80ABEE5E	Generic	USB	USB Attach Device
LAPTOP-10UNBUD9	E:	FBN1701101100024	USB3.0 Flash Disk	USB	USB Remove Device
LAPTOP-10UNBUD9	E:	FBN1701101100024	USB3.0 Flash Disk	USB	USB Attach Device
LAPTOP-10UNBUD9	E:	F6CC3C74	Generic Mass Storage	USB	USB Remove Device
LAPTOP-10UNBUD9	E:	F6CC3C74	Generic Mass Storage	USB	USB Attach Device

- 端點行為包含：程序動作、檔案開啟或修改或刪除、惡意程式、機碼變更、網路連線、作業系統事件、USB插拔、DNS查詢等十餘種類別
- 可查詢到所有端點上發生的事件

查詢到事件後續處理

Investigation / Behaviors

Process Search

Last 30 Days Time: July 12, 2023 09:24:42 - August 11, 2023 09:24:42 Search

er	PID	Name	PPID	Parent Name
AUTHORITY\NETWO...	960	WmiPrvSE.exe	592	svchost.exe
AUTHORITY\SYSTEM	4996	GoogleUpdate.exe	4464	taskeng.exe
AUTHORITY\SYSTEM	4464	taskeng.exe	792	svchost.exe
AUTHORITY\SYSTEM	316	MicrosoftEdgeUpdate.exe	1660	svchost.exe
			592	svchost.exe
			856	svchost.exe
			1748	svchost.exe
			880	svchost.exe
			592	svchost.exe
			592	svchost.exe
			856	svchost.exe

Actions

- Behavior Details
- Parent Details
- Create Detection Rule
- Add Hash to Block List
- Exclude Process from Behavior Collection
- Start Task From Behavior

- 建立自定義Detection Rule，未來發生相同事件就會產生告警
- 直接加黑名單，阻擋下次執行
- 直接加白名單，下次相同事件不再紀錄
- 設定自動反應，當發生特定狀況時指定進行特定工作

設定自動反應作業

New Alert Response

Name: Malware IP Connection Happened and Response

Sources: Fidelis Network, Intelligence Feeds, Process Memory Scan

Severity: Greater than or equal to High

Alert Contains Text: Malicious

Script Package: Logins Failed

Cancel Submit

- 依據告警的類型以及所含的文字敘述，自動執行指定的工作
- 例如：
 - 當發生與惡意IP連線的行為，就自動搜尋登入失敗紀錄，查詢是否被猜密碼
- 預設工作(Task)有150+含各種平台，可自行建立新工作

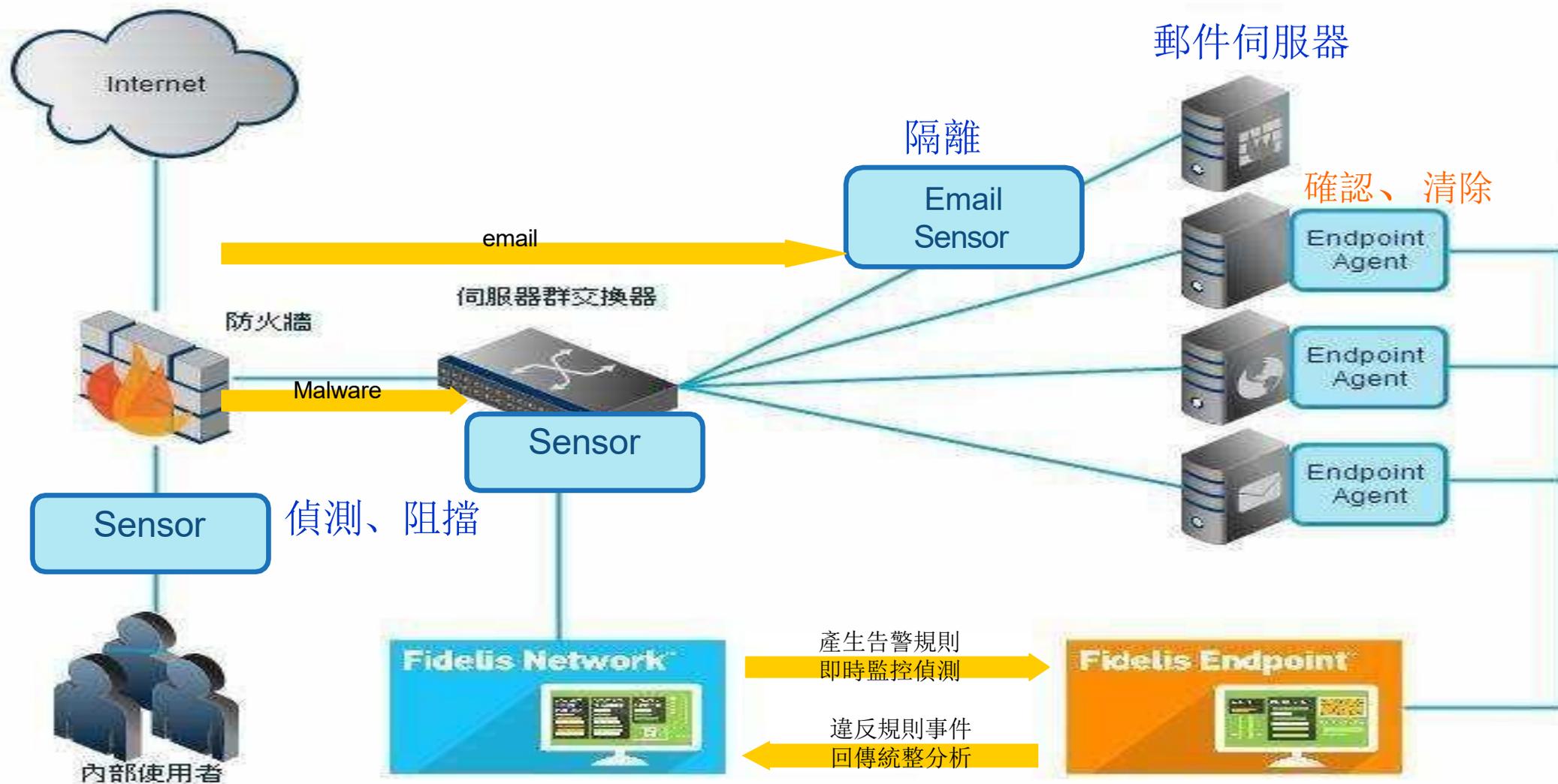


可支援Windows Linux Mac等不同OS平台

OS	Version	Information	
Windows	Windows Server 2016、 2019 Windows 10 Windows 11	Supports 64-bit Supports Behavior Monitoring Supports Antivirus	
Linux	Kernel 3 + CentOS 6, 7 Red Hat Enterprise Linux 6, 7, 8 Ubuntu 14.04, 16.04,18.04, 20.04, 22.04 SUSE Linux Enterprise Desktop 15 Amazon Linux 2017.03 and 2017.09, 2018.03, 2	Supports 64-bit Supports Behavior Monitoring Supports Antivirus (scheduled scan only)	
MacOS	macOS X 10.15 Catalina macOS 11 Big Sur macOS 12 Monterey	Supports Antivirus (scheduled scan only)	

聯防防禦架構

Fidelis聯防系統架構



Network與Endpoint協防

- 增加防禦縱深
- 事件綜合匯整
- 自動建立檢查規則
- 自動回報攻擊確認
- 威脅情資共享
- 單一操作介面

Endpoint Activity



Not Yet Detected



Not Detected



Detected



Blocked



No Agent

Deception與Endpoint/Network的聯防

- Deception誘捕系統運作原理
 - Network收集網內的網段架構
 - 端點/伺服器的服務
 - 自動佈署相同的誘餌端點來引誘駭客入侵
- Deception資料均匯整於Network介面，單一平台統合
- Endpoint/Network發現疑端點被入侵，Deception提供確認是否被compromise
- 改善告警正確率

總結



結語

- Endpoint-最強端點管理能力清除
 - 能力最強
 - CP值最佳(內建防毒軟體)
 - 支援最多種平台(Win、Linux、Mac)
 - 調查速度最快(事件集中式管理)
 - 防禦縱深最長(整合Network協同作業)
 - 可阻止勒索軟體



Thank you

TM