

原芬-安全企業版 Formerly F-Secure Business

WithSecure™

唯思安全®

Elements Endpoint Protection (EPP)

雲中控端點安全解決方案

Elements Endpoint Detection and Response (EDR)

端點偵測與響應解決方案



台灣總代理 | 湛揚科技
www.t-tech.com.tw



A comprehensive solution to fit your needs

滿足您企業所有需求的全面解決方案

Contents

一、關於WithSecure™ 唯思安全® (原芬-安全企業版，Formerly F-Secure Business)	2
二、WithSecure™ Elements Endpoint Protection 唯思安全® 雲中控端點安全解決方案	3
三、WithSecure™ Elements Endpoint Detection and Response 唯思安全® 端點偵測與響應解決方案	8

明日的安全，今日就緒 Tomorrow's security, delivered today.

網路安全永無止境，每天都會出現新的攻擊手法和層出不窮的威脅，駭客永遠都不會停止挖掘及部署新方法來突破您的防禦，這意味著不能放慢速度，您不會想成為駭客的下一個目標，這就是使網路安全變得有趣和無情並且充滿挑戰的原因。

挑戰是趨動我們向前的力量！ We are driven by that challenge!

WithSecure™ 孜孜不倦地研發，以領先競爭者一步，我們瞭解網路安全並且堅持不懈，為表彰我們的成功，我們連續多年榮獲AV-Test頒發享有盛譽的“最佳保護”獎，而這僅是證明我們提供現在和未來最佳安全性的眾多證據之一。



一、關於WithSecure™ 唯思安全® (原芬-安全企業版, Formerly F-Secure Business)

WithSecure™ 唯思安全® 是一家歐洲資訊安全公司前身為芬-安全F-Secure企業版, 擁有數十年的經驗, 致力於保護企業免受機會主義勒索軟體感染到進階資訊攻擊等各種威脅。透過WithSecure™ 唯思安全® 的安全創新專利和複雜的威脅情報, 讓我們的全面服務和屢獲殊榮的產品, 保護著數以萬計的公司和數百萬人。

WithSecure™ 唯思安全® 的資訊安全專家參與了比市場上任何其他公司更多的歐洲資訊犯罪現場調查, 我們的產品由數千名經銷商和數百名運營商在全球範圍內銷售, 並於 2017 年授權湛揚科技為台灣總代理。

現今企業環境及需應付的威脅

當今的企業環境正在不斷且迅速地演變, 網路威脅也是如此, 雖然各行各業都在向雲端遷移並採用新的數位化工作方式, 但攻擊者正在透過更先進、更有效的方法不斷擴大攻擊層面, 因此應對新威脅的常見方式為從多家供應商組合一套複雜的技術解決方案, 但這種複雜的解決方案組合, 不僅在操作上或管理上都相當的複雜, 而且還會在您的資訊安全裡留下漏洞。

WithSecure™ Elements 的優點

WithSecure™ Elements提供靈活的一體化安全平台, 可適應企業和威脅格局的變化, 它是一個統一的雲端原生平台, 涵蓋安全價值鏈的所有關鍵領域: 端點保護、端點檢測和回應、弱點管理以及對Microsoft 365的保護, 如此一來您就可以靈活選擇互補的技術和解決方案。

最強而有力的解決方案 A powerful solution



二、WithSecure™ Elements Endpoint Protection 唯思安全® 雲中控端點安全解決方案(EPP)

支援繁體中文

雖然各行各業都邁向雲端和數位化工作方式，但攻擊者不斷擴大攻擊層面，因此常見從多家供應商組合一套複雜的解決方案，但這樣不僅在操作上或管理上都相當複雜，而且還很容易留下弱點。WithSecure™ Elements 唯思安全® 雲端防護解決方案為公司提供 all-in-one 的安全防護，可適應企業和威脅格局的快速變化，WithSecure™ Elements 唯思安全® 雲端防護解決方案將一系列涵蓋安全價值鏈的所有關鍵領域，包括端點保護、檢測和響應，整合成一個全方位的軟體，並能夠在一個統一的雲端中控台進行管理，包括個人電腦及筆電的安全防護、行動裝置安全防護、伺服器安全防護以及雲端中控管理平台。



個人電腦及筆電的安全防護 Computer Protection

強大、多層式的安全性，適用於Windows和Mac。

- 包括Windows電腦的修補程式管理
- 使用進階行為和啟發式分析
- 利用人工智慧和機器學習
- 保護 Salesforce 雲端環境的使用者



行動裝置安全防護 Mobile Protection

防止iOS和Android行動裝置上的惡意軟體和資料遺失。

- 保護設備免受惡意軟體和網路釣魚的侵害
- 防止資料因被盜用，設備和 Wi-Fi 窺探而丟失
- 提供第三方MDM支援



伺服器安全防護 Server Protection

保護您的關鍵任務通信、協作和資料儲存。

- 專為伺服器設計的新世代防護
- 進階行為分析和啟發式分析
- 完全整合的修補程式管理
- 遠端管理防火牆
- 應用程式和裝置控制



雲端中控台管理平台 Management Portal

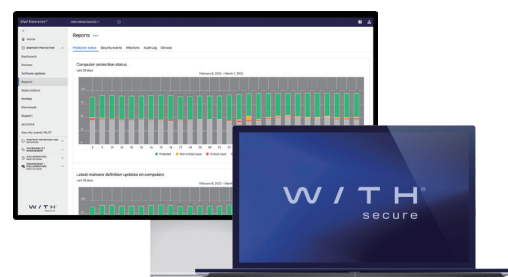
透過單一且基於雲端中控台部署、管理和監控一切。

- 整合修補程式管理
- 無需伺服器硬體
- 第三方管理工具的完全整合

個人電腦及筆電的安全防護 Computer Protection

WithSecure™ Elements Endpoint Protection 為您的Mac*和Windows端點提供強大且符合當下的安全性，藉助透過WithSecure™安全雲提供的修補程式管理和實時威脅情報等工具，您的安全性將提升到一個全新的水準。同時也設計適用於保護Mac電腦的安全性。

支援的操作系統：Windows 7 SP1、8.1、10、11 / macOS Apple 10.15、11、12



先進的惡意軟體防護 Advanced anti-malware

提供多引擎檢測能力。提供比傳統解決方案更好的安全性，而不依賴於單一技術。

W / T H secure			
Security Outcomes Solutions Expertise Partners Get Support			
CLIENT SECURITY, PS8 PRODUCTS, SAFE FOR WINDOWS 32-BIT			
Date	Package	Version	Size
2023-06-08 05:54 UTC	F-Secure Capricorn	2023-06-08_04	130.68 MiB
2023-06-08 03:39 UTC	F-Secure DeepGuard DB	2023-06-08_01	1.02 MiB
2023-06-07 09:16 UTC	F-Secure Hydra	2023-06-07_01	15.29 MiB
2023-05-25 08:05 UTC	F-Secure Ultralight Core	2023-05-25_01	20.30 MiB
2023-05-22 13:45 UTC	F-Secure Virgo	2023-05-22_01	2.14 MiB
2023-04-25 13:43 UTC	F-Secure Ultralight Updater	2023-04-25_01	3.42 MiB

資料防禦技術 DataGuard **

提供針對勒索軟體的額外檢測功能，並防止破壞和篡改資料。



網頁防護 Web protection

防止瀏覽惡意和網路釣魚網站，阻止惡意腳本和內容，並為關鍵業務網路活動提供更高的保護。



*可用功能因操作平台而異

**進階版功能

深藍引擎 DeepGuard

透過使用啟發式和行為分析，針對零時差攻擊和漏洞利用攻擊提供主動保護。



應用程式控制 Application control**

根據我們的滲透測試人員創建的規則或管理員定義的規則阻止應用程式和腳本的執行。



安全雲 Security cloud

我們的威脅分析和回應系統為我們的客戶提供實時威脅情報，使他們能夠在新威脅出現時識別和回應。

裝置控制 Device control

啟用對基於USB的設備控制，防止資料丟失和透過它們感染惡意軟體。

修補程式管理 Patch management

透過自動修補Windows和第三方軟體漏洞，阻止高達 80% 的攻擊，其功能包括排除、手動更新選項。

 行動裝置安全防護
Mobile Protection

WithSecure™ Elements Endpoint Protection 為您提供了一種簡單的方法來保護和控制您的行動裝置，包括iOS和Android，無論在何處，您可在一個組件中獲得所需的一切：Wi-Fi 保護、瀏覽保護、行動裝置管理支援和 VPN。

支援的作業系統：iOS 12.1 及更高版本 / iPadOS 13及更高版本 / Android 7.0 (Nougat) 及更高版本



行動装置 VPN Mobile VPN

自動加密 (VPN) 行動裝置和選定的WithSecure™服務節點之間的所有流量，允許安全使用公共Wi-Fi和行動網路。(如圖1)

瀏覽保護 Browsing protection

在瀏覽之前預警，並防止使用者瀏覽惡意網站和釣魚網站。(如圖2)

■ 高效輕量的防護軟體 Ultralight anti-malware

當 VPN 處於活動狀態時，我們的服務節點會保護手機免受惡意軟體和惡意內容的侵害。

輕量沒負擔的代理程式 Lightweight client

強大的安全功能在雲端處理，確保對行動裝置性能和電池壽命的影響最小。

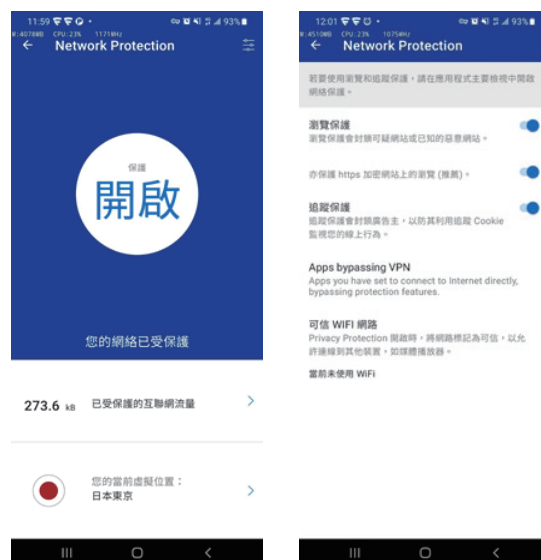
設備狀態 Device status

提供有關設備的詳細信息，例如易受攻擊的操作系統版本以及它們是否已植入Root。

[illegible]

支援行動裝置管理 External MDM

支援透過第三方MDM解決方案進行部署，例如 AirWatch、MobileIron、Intune 和 MaaS360。

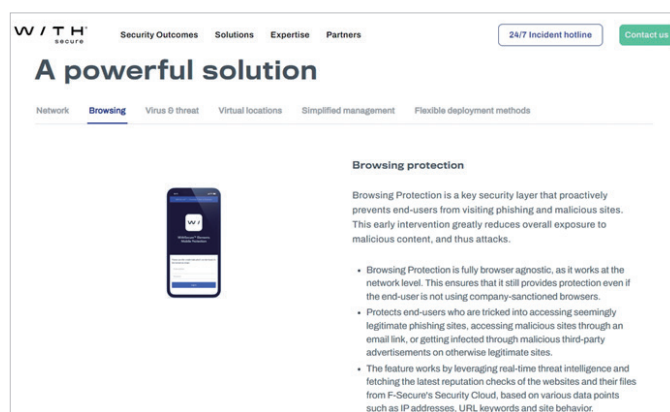


(圖1)

(圖2)

| 安全雲 Security cloud

我們的威脅分析和回應系統為我們的客戶提供實時威脅情報，使他們能夠在新威脅出現時識別和回應。



高速瀏覽 Faster browsing

透過使用流量壓縮和阻止資源密集型線上追蹤和廣告，將瀏覽速度提高多達30%。

伺服器安全防護 Server Protection

WithSecure™ Elements Endpoint Protection 為您的伺服器提供最高的安全性，同時保持它們以最佳性能運行。

支援的平台*：Microsoft Windows Server 2008 R2 SP1 作業系統及更高版本 / Microsoft Windows Terminal Server / Citrix Server / Linux Server



進階防惡意軟體 Advanced anti-malware

先進的防惡意軟體平台，使用多引擎檢測功能，在不依賴單一技術的情況下提供更好的安全性。

CLIENT SECURITY, PSB PRODUCTS, SAFE FOR WINDOWS 32-BIT			
Date	Package	Version	Size
2023-06-08 05:54 UTC	F-Secure Capricorn	2023-06-08_04	130.68 MiB
2023-06-08 03:39 UTC	F-Secure Deepguard DB	2023-06-08_01	1.02 MiB
2023-06-07 09:16 UTC	F-Secure Hydra	2023-06-07_01	15.29 MiB
2023-05-25 08:05 UTC	F-Secure Ultralight Core	2023-05-25_01	20.30 MiB
2023-05-22 13:45 UTC	F-Secure Virgo	2023-05-22_01	2.14 MiB
2023-04-25 13:43 UTC	F-Secure Ultralight Updater	2023-04-25_01	3.42 MiB

修補程式管理 Patch management

涵蓋2500多種伺服器和第三方軟體，例如Apache、BizTalk、Microsoft SQL、Flash、java等。

針對 Windows 伺服器的設定檔		已指定伺服器: 1 上次編譯時間: 2023/1/30 上午11:42 設定檔 ID: 45620479	...
軟體更新程式			
所有設定檔設定			
在此輸入以搜尋特定設定...			
一般設定	軟體更新程式	開啟	
即時掃描	本機使用者介面	開啟	
手動掃描	自動掃描以查看是否存在缺失更新	開啟	
置換保護	掃描優先順序	幕後	
防火牆	僅安裝已簽名的更新	關閉	
軟體更新程式	通知新的缺失更新	開啟	
裝置控制	自動安裝		
自動任務			
網路位置設定			

對 Citrix 環境的額外保護 Protection

已透過Citrix認證可添加完整的安全堆棧支援，為已發布的應用程式添加修補程式管理支援，在與Windows伺服器相同的核心安全功能之上，Citrix組件通過擴展已發布應用程式的集成補丁管理功能，為Citrix環境提供額外的保護，該客戶端已通過Citrix Ready認證，確保它在Citrix環境中完美運行。

安全雲 Security cloud

我們的威脅分析和回應系統為我們的客戶提供實時威脅情報，使他們能夠在新威脅出現時識別和回應。

Connectivity status		Connected
Connectivity status shows potential problems with the Security Cloud connection. Successful connections are not listed.		
- A connection issue may happen randomly. You can ignore the "Not always connected" status if there are no visible issues. - The status is updated once per day or when a full status update is requested. - An unused URL is removed from the connectivity status after ten days of inactivity.		
Make sure that the connections to *.f-secure.com and *.fapi.com are allowed in your network.		
Connectivity status		Not always connected
Connectivity status shows potential problems with the Security Cloud connection. Successful connections are not listed.		
- A connection issue may happen randomly. You can ignore the "Not always connected" status if there are no visible issues. - The status is updated once per day or when a full status update is requested. - An unused URL is removed from the connectivity status after ten days of inactivity.		
Make sure that the connections to *.f-secure.com and *.fapi.com are allowed in your network.		
poll-push-apac.fapi.com	Not always connected. There were a few failed requests but the service is working.	
psb-apac.dooman.fapi.com	Not always connected. There were a few failed requests but the service is working.	

深藍引擎 DeepGuard

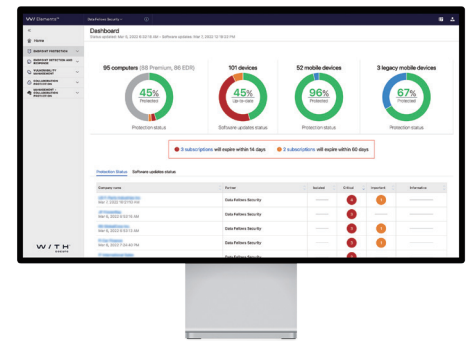
透過使用啟發式和行為分析，針對零時差惡意軟體和漏洞利用提供主動保護。

針對 Windows 伺服器的設定檔		已指定伺服器: 1 上次編譯時間: 2023/1/30 上午11:42 設定檔 ID: 45620479	...
無防線的應用程式			
DeepGuard		開啟	
此設定開啟 DeepGuard 保護。我們強烈建議您將 DeepGuard 保持開啟，因為它提供可抵禦未知勒索軟體等的關鍵保護。			
DeepGuard 提供/關閉，將開啟/關閉以下保護：			
開啟/關閉 - DeepGuard			
開啟/關閉 - 入侵程式防護			
開啟/關閉 - 勒索軟體防護			
開啟/關閉 - 微變式分析			
開啟/關閉 - 行為監視			
封鎖可疑和可疑的檔案		開啟	
DeepGuard 保護規則			
已啟用	應用程式 SHA-1	注釋	信任
無 DeepGuard 保護規則			

WithSecure™ Elements 安全管理中心 WithSecure™ Elements Security Center

WithSecure™ Elements Endpoint Protection所有內容皆可在雲端一個中控台進行管理，包括部署、管理和監控所有端點安全組件、配置文件和整合工具，為您節省管理和維護的寶貴時間。

支援的瀏覽器：最新版本 Microsoft Edge、Mozilla Firefox、Google Chrome、Safari



集中管理 Centralized management

將所有端點組件和整合工具的管理整合到雲中控台中統一管理。

裝置類型	名稱	安裝日期	OS 版本	WithSecure™ 產品名稱	安裝日期	OS 版本	安裝日期	安裝日期	安裝日期	安裝日期
Windows	10000000000000000000	Sep 27, 2022	CentOS	WithSecure™ for Linux	Sep 27, 2022, 5:10:00 PM	12.0.10	已安裝	已安裝	已安裝	已安裝
Windows	10000000000000000000	Jun 15, 2022	Windows Server 2016	WithSecure™ Server	Aug 4, 2022, 2:41:08 PM	22.4	已安裝	已安裝	已安裝	已安裝
Windows	10000000000000000000	May 15, 2022	Windows 11	WithSecure™	Jun 16, 2022, 1:10:53 PM	22.2	已安裝	已安裝	已安裝	已安裝
Windows	10000000000000000000	Jun 29, 2022	Windows 11	WithSecure™	Oct 31, 2022, 2:01:05 PM	22.7	已安裝	已安裝	已安裝	已安裝
Windows	10000000000000000000	Jun 16, 2022	Windows 11	WithSecure™	Apr 16, 2022, 1:05:02 PM	22.1	已安裝	已安裝	已安裝	已安裝
Windows	10000000000000000000	Jul 12, 2022	Windows 10	WithSecure™	Oct 30, 2022, 1:10:53 PM	22.7	已安裝	已安裝	已安裝	已安裝
Windows	10000000000000000000	Feb 18, 2021	Windows 7	WithSecure™ Office (paid)	Sep 16, 2022, 6:21:11 PM	22.5	已安裝	已安裝	已安裝	已安裝
Windows	10000000000000000000	Apr 20, 2020	Windows Server 2019	WithSecure™ Server	Oct 11, 2022, 1:10:53 PM	22.7	已安裝	已安裝	已安裝	已安裝

託管管理入口網站 Hosted management portal

完美符合Html 5，無需安裝管理伺服器或特殊軟體，適用於任何裝置與設備。

Logname	Email	Computers & mobile devices	Services	Last logged in
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM
admin	admin@withsecure.com	Full editing	Full editing	Jun 15, 2022 10:16:44 AM

自動化更新 Automatic updates

在管理平台和客戶端自動部署產品、安全和資料庫更新，減少人工維護工作的時間。

軟體更新	更新日期	更新內容	更新狀態	更新日期	更新內容	更新狀態	更新日期	更新內容	更新狀態
Microsoft Corporation	2022-08 Security Update for Windows Server 2019 for x64-based Systems (KB5013270)	是	是	2022-08-10	KB5013270	已安裝	2022-08-10	KB5013270	已安裝
Microsoft Corporation	2021-08 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB5005112)	是	是	2021-08-10	KB5005112	已安裝	2021-08-10	KB5005112	已安裝
Microsoft Corporation	2020-11 Cumulative Update for Windows 10 for x64-based Systems (KB4567890)	是	是	2020-11-10	KB4567890	已安裝	2020-11-10	KB4567890	已安裝
Microsoft Corporation	2020-10 Security Update for Active Directory for Windows 10 Version 1809 for x64-based Systems (KB4567890)	是	是	2020-10-10	KB4567890	已安裝	2020-10-10	KB4567890	已安裝
Microsoft Corporation	Security Update for Microsoft Office 2016 (KB4567890) 64-bit Edition 15.0.15044	是	是	2020-10-10	KB4567890	已安裝	2020-10-10	KB4567890	已安裝

卸載工具 Uninstallation tool

在部署Windows客戶端期間會自動刪除衝突的安全解決方案，確保順利過渡。

卸載工具

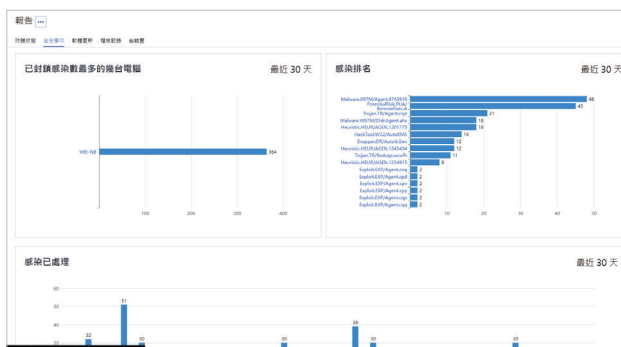
如果正常卸載方法失敗，該工具可從您的 Windows 計算機中刪除 WithSecure 產品。

適用於 Business Suite、電子郵件和服務器安全、計算機的 Elements EPP 以及 Elements 端點檢測和響應產品。

下載 [自述文件](#)

廣泛報告 Extensive reporting

詳細的圖形化報告，例如帶有威脅詳細信息的“受攻擊最多的用戶端”、基於缺失修補程式的漏洞報告等。



提供管理與第三方軟體協作的 API Management API

支援透過API整合到SIEM、RMM或任何其他第三方審查、管理或報告工具。

WithSecure™ 元素 API

對於更深入的集成，WithSecure™ 為合作夥伴提供了許多公共 API：

端點保護 API

一種多用途 API，用於管理計算機、監視事件、列出訂閱、控制各種端點保護功能以及生成報告。

[入門](#)
[API 參考](#)

漏洞管理 API

我們的漏洞管理解決方案公開的 API，允許以編程方式訪問幾乎所有產品功能。

[入門](#)
[API 參考](#)

供應 API

用於 WithSecure™ 合作夥伴的 API，用於自動配置 WithSecure™ Elements 訂閱，包括基於使用的安全策略模型。

[入門](#)
[API 參考](#)

易於部署 Easy deployment

端點安全客戶端可以透過電子郵件、本地安裝、批次腳本或基於網域的遠端安裝工具進行部署。

政策設定 Policy setting

可以使用單獨標籤或分組創建、自定義和分配安全策略。

三、WithSecure™ Elements Endpoint Detection and Response 唯思安全® 端點偵測與響應解決方案(EDR)

WithSecure™ Elements Endpoint Detection and Response 唯思安全® 端點檢測和響應是 Elements 網路安全平台的一個模組。基於雲端的平台提供了針對勒索軟體和高級攻擊的有效保護。Elements 將漏洞管理、漏洞修補管理、動態威脅情報和持續行為分析結合在一起。您可以針對特定的需求使用單獨的解決方案，或組合它們以實現最大程度的防禦。

如果能看見威脅，就能阻止

從單一控制台管理您所有的安全需求。WithSecure™ Elements 唯思安全® 解決方案為您提供能適應不斷變化的威脅和業務上所需的清晰度、靈活性和技術。

為何選擇 WithSecure™ Elements Endpoint Detection and Response 唯思安全® 端點偵測與響應解決方案？

1 提高可見性

透過應用程式和端點清單提高對IT環境狀態和安全性的可見性。並透過收集和關聯惡意軟體之外的行為事件，輕鬆發現是否正確使用。

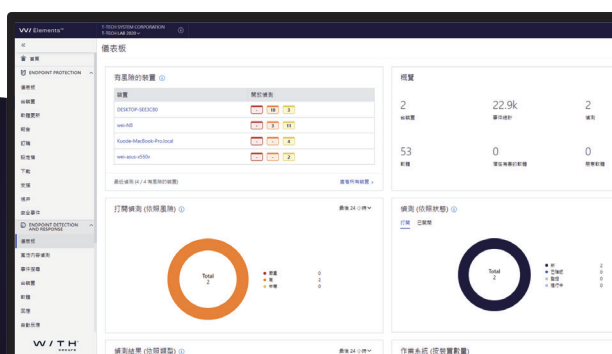
2 快速偵測弱點

具備最少誤報的即時警報，可快速偵測具針對性的攻擊，透過在短時間內設定高級威脅偵測和回應功能，在發生違規行為先一步做好準備。

3 受到攻擊時快速回應

透過內建自動化和人工智慧提高團隊的注意力，支援對真正高級威脅和有針對性的攻擊做出快速回應，並獲取如何使用全年無休自動回應的指導。

最強而有力的
EDR解決方案



廣泛關聯偵測™ Broad Context Detection

針對性攻擊的廣泛關聯，可在時間軌跡上立即可見，包含所有受影響的主機，相關事件和建議措施。該解決方案是根據即時行為、信譽和大數據分析，將風險等級，受影響主機的重要性的當時的威脅環境，透過機器學習做自動偵測並將結果置於廣泛關聯偵測內。

自動回應 Automated Response

只要風險級別足夠高，就可以透過全天候控制目標的網路攻擊，使用自動回應措施來減少目標網路攻擊的影響。根據預定義的時間表，此自動化系統專門設計用於支持僅在工作時間內可用的團隊，同時也考慮了偵測的重要性。

事件搜索 Event Search

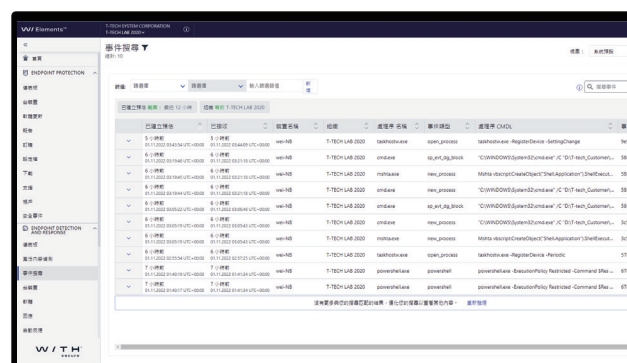
借助此內置功能，您可以查看和探索從與任何廣泛關聯偵測相關的公司端點收集的事件資訊。此高級應用功能用於探索從端點收集的所有原始事件資訊並與之交流。其先進的過濾功能讓 SOC 的網路安全專家執行主動威脅搜尋，以偵測和阻止最複雜的隱藏威脅。威脅搜尋的事件搜索是 WithSecure™ Elements 端點偵測和回應的選擇組件。

提升至 WithSecure™ Elevate to WithSecure™

有些偵測需要專業的網路安全專家進行更深入的威脅分析和指導。對於這些困難的情況，該解決方案內建了獨特的服務「提升至 WithSecure™」。它提供了廣泛的方法和技術，網路路由，流量來源以及 Broad Context Detection™ 時間表的專業事件分析，可在受到攻擊時提供專家的建議和進一步的回應指導。

主機隔離 Host isolation

儘早停止違規是至關重要的，並且透過主機隔離，可以實現這一目標。當偵測到弱點時，可以自動或手動將受影響的主機與網路隔離，從而阻止攻擊者使用主機。同時 IT 安全專家可以對主機進行調查，以獲取有關破壞的線索。即便主機受到隔離，仍可從管理門戶進行集中管理。



關於湛揚科技

湛揚科技是 WithSecure™ 唯思安全® 企業防毒產品與芬-安全F-Secure個人防毒產品台灣總代理，成立於2005年，湛揚科技始終致力於協同合作夥伴提供『資料保護，端點安全及虛擬設備防護』等高性價比產品代理及專業服務為公司宗旨。湛揚科技同時也是Acronis 安克諾斯® 台灣總代理，提供通路夥伴及企業客戶資安基礎建設必備項目－『新世代備份、防毒、雲服務』。在未來千變萬化的網路應用與建置的環境下，透過最佳解決方案提供自動化防護，偵測及回應的新數位安全時代，並以達成『客戶滿意』為企業使命及目標。



EPP+EDR 電子型錄下載

總代理

WithSecure™
www.t-tech.com.tw

湛揚科技

台北：(02)2515-1585
南區：(07)972-7388