Acronis

#CyberFit

Cyber Protect Cloud

AI 智能 自動進化超融合多層次防護

雙總部
分別位於瑞士和新加坡

Acronis資訊安全领先者- Cyber Protect Cloud

全球五十萬企業好級客戶 五百五十萬中小企業客戶 覆蓋150國家 35個數據中心 4座全球情資中心

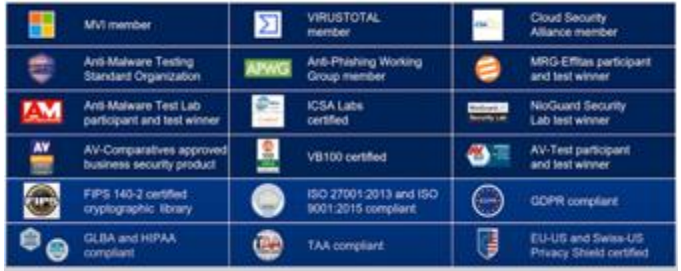
FORTUNE 1,000

Protect By Acronis

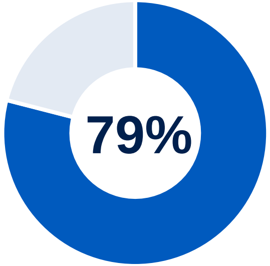
S A P A S

領先業界的資安認證測試

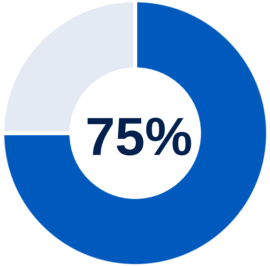
Security Industry Recognitions



MVI member	VIRUSTOTAL member	Cloud Security Alliance member
Anti-Malware Testing Standard Organization	APWG Anti-Phishing Working Group member	MRG-Effitas participant and test winner
AM Anti-Malware Test Lab participant and test winner	ICSA Labs certified	NioGuard Security Lab test winner
AV AV-Comparatives approved business security product	VB100 certified	AV-Test participant and test winner
FIPS 140-2 certified cryptographic library	ISO 27001:2013 and ISO 9001:2015 compliant	GDPR compliant
GLBA and HIPAA compliant	TAA compliant	EU-US and Swiss-US Privacy Shield certified



of **Top100** Most Valuable Brands



of Tech **Top20**

北美區 200,000+ 企業級客戶

IBM Pfizer hp HBO 3M GM
MARS Honeywell LOCKHEED MARTIN
EXXON Mobil Chevron MARATHON Schlumberger

歐洲區 200,000+ 企業級客戶

Audi TOTAL OXFORD Unilever AIRBUS Shell
TESCO orange LEGO BASF The Chemical Company Deutsche Bank PHILLIPS 66
ConocoPhillips bp

亞太區 100,000+ 企業級客戶

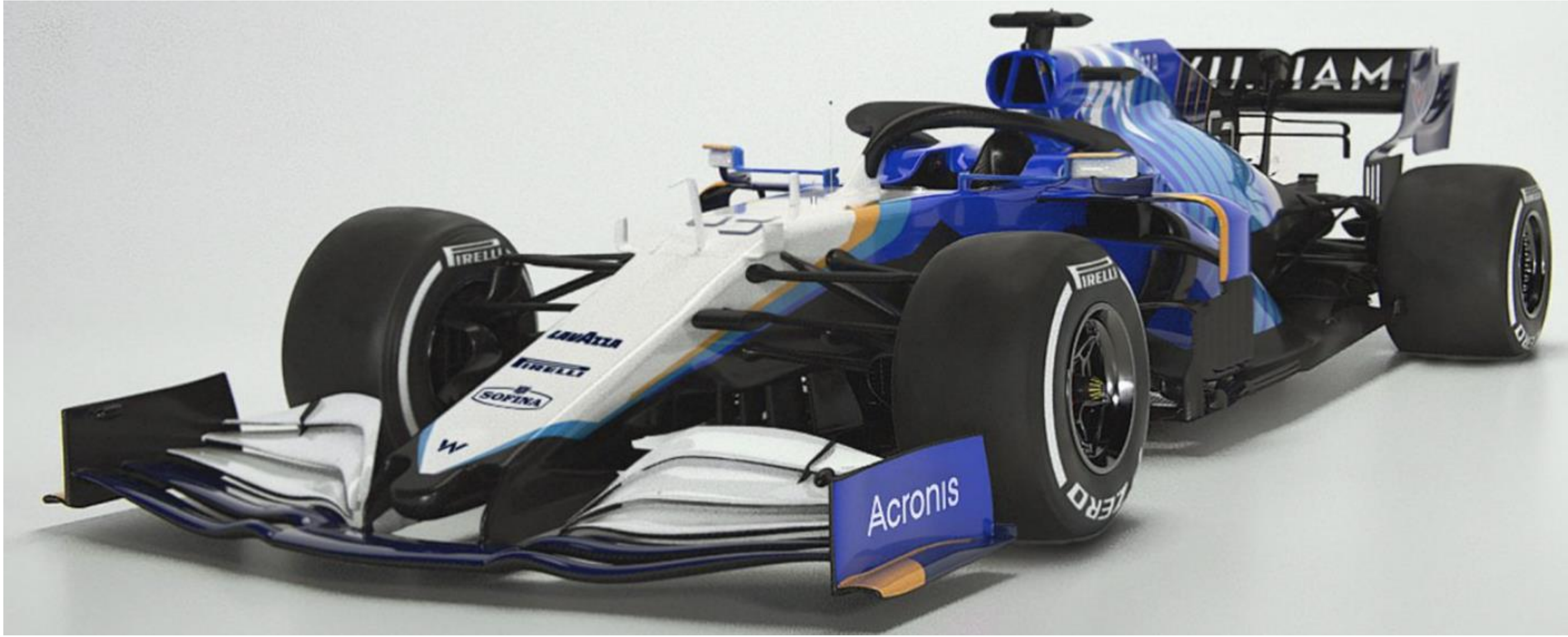
SINGAPORE POWER Panasonic NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE NUS National University of Singapore
SONY PETRONAS Singtel NEC brother
Valero

Acronis

雙總部
分別位於瑞士和新加坡

#CyberFit

Williams車隊2021年新賽車FW43B現真身



06:45.900
Nürburgring Nordschleife
NIO eP9
为超越极限而生
Born to Push Limits
Formula E
Team
Julius Bär
Acronis
NIO 333 RACING
MICHELIN
8
OLIVER TURVEY
NIO 333 FE Team
NIO

NIOHouse | Auto Shanghai

ADVANTECH
研華科技
tsmc
國泰人壽
Cathay Life Insurance
Synology
群暉科技
QNAP
威聯通科技
玉山銀行
CHB
CHANG HWA BANK
彰化銀行
凱基銀行
KGI BANK
DBS
星展銀行
正新橡膠
We are Family
中國信託銀行
CTBC BANK
台灣大哥大
Taiwan Mobile
台灣高鐵
TAIWAN HIGH SPEED RAIL
凌陽科技
TCE
中華凸版電子股份有限公司
TOPPAN CHUNGHWA ELECTRONICS
中華民國外交部
MINISTRY OF FOREIGN AFFAIRS
REPUBLIC OF CHINA (TAIWAN)

*全球頂尖**F1**賽事,美國職棒,歐洲足球聯賽,日本頂尖賽車 採用**Acronis***

More than 50 teams use Acronis tech

資安威脅態勢越來越複雜

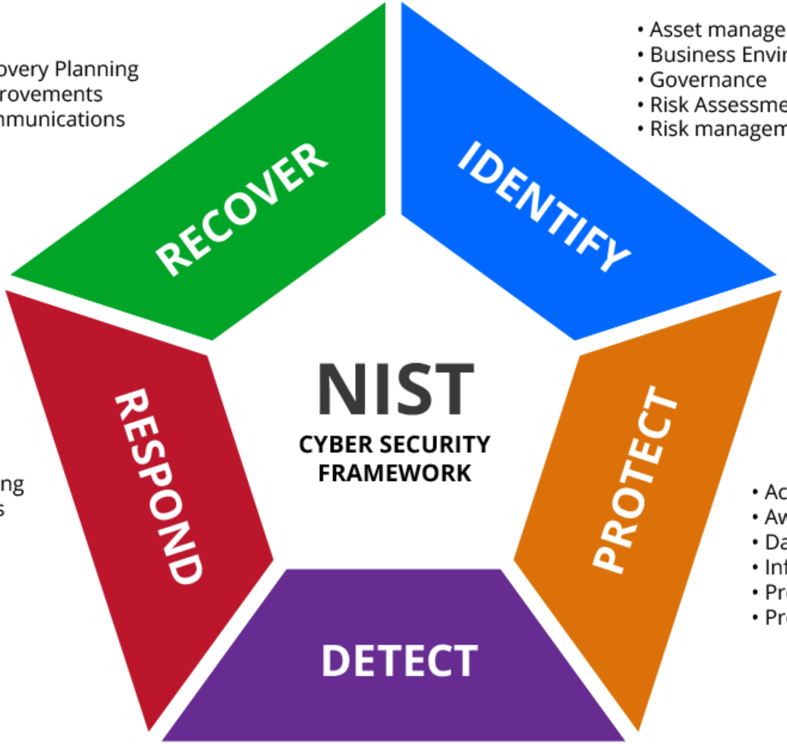
COVID-19 疫情
期間網路犯罪活動突增
300%

傳統
防毒解決方案會使 57%
的攻擊成為漏網之魚

69% 的人
花費更多時間來管理工具
而非抵禦威脅

來源：2020 年 Acronis 網路威脅報告、FBI 2020 年 Acronis 網路整備性報告

NIST 建議企業根據資安框架檢視資安管控



- Recovery Planning
- Improvements
- Communications

- Asset management
- Business Environment
- Governance
- Risk Assessment
- Risk management Strategy

- Response Planning
- Communications
- Analysis
- Mitigations
- Improvements

- Access control
- Awareness training
- Data Security
- Information protection
- Processes and Procedures
- Protective technology

- Anomalies and Events
- Security continuous monitoring
- Detection processes

資安與資料保護痛點與挑戰

買了這麼多的資安產品，您覺得自己安全嗎？

居家辦公，是否擔心勒索軟體攻擊及資料外洩？

資安架構該如何規劃，才能達到安全、簡單、有效?

都有做備份，但備份的資料是乾淨無毒的嗎?

使用家裡電腦居家辦公，安全嗎？有什麼簡單的方式改善?

備份資料還原後，會擔心重複感染嗎?

企業都有防毒軟體，勒索攻擊還是很多，您擔心成為受害者嗎?

台灣企業對勒索軟體的防禦力？

- ➢企業買了這麼多的資安產品，您覺得真的安全了嗎？
- ➢企業備份的資料是安全乾淨的嗎？
- ➢系統復原後擔心會再重覆感染嗎？

傳統防護產品已經無法成功抵禦現今之勒索軟體攻擊

- ➢ 自2017 年以來，勒索軟體除了加密資料外，都開始攻擊企業的備份解決方案，讓備份失效，確保勒索成功。
- ➢ 且勒索軟體攻擊平均潛伏期為 90 – 180 天，攻擊進程利用很多漏洞進行推進，以確保最後勒索成功，
- ➢ 因此從 NIST 資安防護架構進行檢視，將企業有限之資源應用在最大效益之防護，簡單分為以下幾個防護面向 ：

- 事前預防：企業透過精簡的集中管控機制、弱掃及自動化漏洞修補程序，節省時間及人力。
- 事中防護：零時差主動偵測及自動復原機制，企業不需再擔心新的勒索病毒變種威脅。
- 事後回復：事後安全回復機制，確保備份資料乾淨復原，企業不會再遭受二次感染。
- V

資訊安全規劃

減少孤島 整合式 智能化 連動聯防平台

事前預防

- 關鍵思考

- 事前預防的關鍵, 資安管理; 尤其是即時Patch 管理
- 業界平均是102天;安全等級高的需要34天
- 中間的空窗期,攻擊的關鍵
- 但是, 另一個挑戰,一年有超過1萬五千多個CVE要補漏洞
- 怎麼發現這些漏洞要補

事中防護

- 建置多種資安工具,但是彼此不聯防連動

- 業界太多種資安工具, 資安人員無法有效選擇, 有時還造成彼此衝突
- 更進一步分析，資安工具實際使用並未達到應有防禦設定
- 缺乏資安顧問做全面性架構建議和規劃
- 缺乏整體資安管理和情資訊息

事後回復

- 資料備份和資安工具獨立

- 駭客潛伏超過180天
- 你怎麼確定備份的資料是乾淨的
- 真的遭受攻擊後,要從備份復原,怎麼避免重複受到感染和攻擊
- 勒索軟體針對主機,備份和異地雲設備都進行攻擊,怎麼辦？
- 怎麼發現攻擊手法和路徑

Cyber Security Challenges

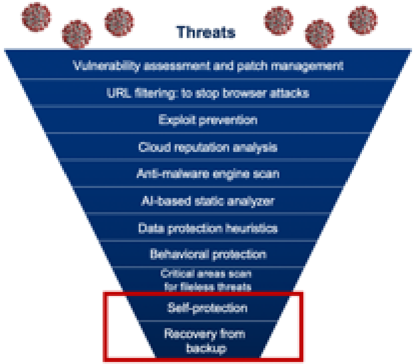
缺乏完整資安架構規劃

資安產品太分散 無法聯防連動 無法有效防禦

威脅手法 日新月異 資安人才和技能嚴重不足

新型態防禦架構- 資安和復原整合技術

CYBER SECURITY + DATA PROTECTION

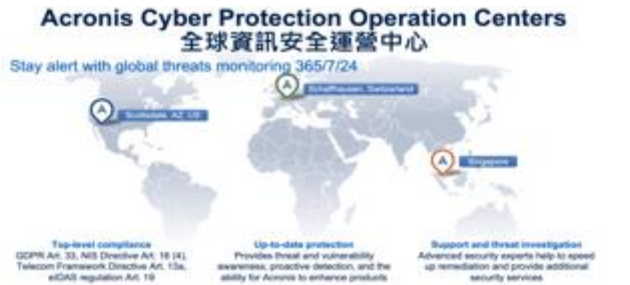

Threats
Vulnerability assessment and patch management
URL filtering: to stop browser attacks
Exploit prevention
Cloud reputation analysis
Anti-malware engine scan
AI-based static analyzer
Data protection heuristics
Behavioral protection
Critical areas scan for fileless threats
Self-protection
Recovery from backup

HOW WE HELP YOU? ACRONIS

防禦鐵三角

全球運營情資中心-及時響應防禦政策

CPOC(Cyber Protection Operation Center)


Acronis Cyber Protection Operation Centers
全球資訊安全運營中心
Stay alert with global threats monitoring 365/7/24
Scottsdale, AZ, US
Schaffhausen, Switzerland
Singapore

Top-level compliance
GDPR Art. 33, NIS Directive Art. 16 (4), Telecom Framework Directive Art. 13a, eIDAS regulation Art. 19

Up-to-date protection
Provides threat and vulnerability awareness, proactive detection, and the ability for Acronis to enhance products

Support and threat investigation
Advanced security experts help to speed up remediation and provide additional security services

整合式顧問服務-企業營運不中斷規劃

Cyber Security and Data Protection Consultant

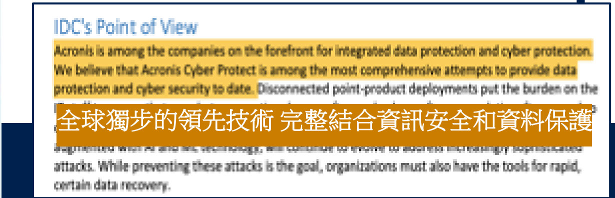
Safety
資訊保護
Nothing is lost: there is always a copy for recovery

Accessibility
存取安全
Access from anywhere at any time

Privacy
隱私保護
Control over visibility and access

Authenticity
認證保障
Proof that a copy is an exact replica of the original

Security
資訊安全
Protection against bad actors



IDC's Point of View

Acronis is among the companies on the forefront for integrated data protection and cyber protection. We believe that Acronis Cyber Protect is among the most comprehensive attempts to provide data protection and cyber security to date. Disconnected point-product deployments put the burden on the [illegible]

全球獨步的領先技術 完整結合資訊安全和資料保護

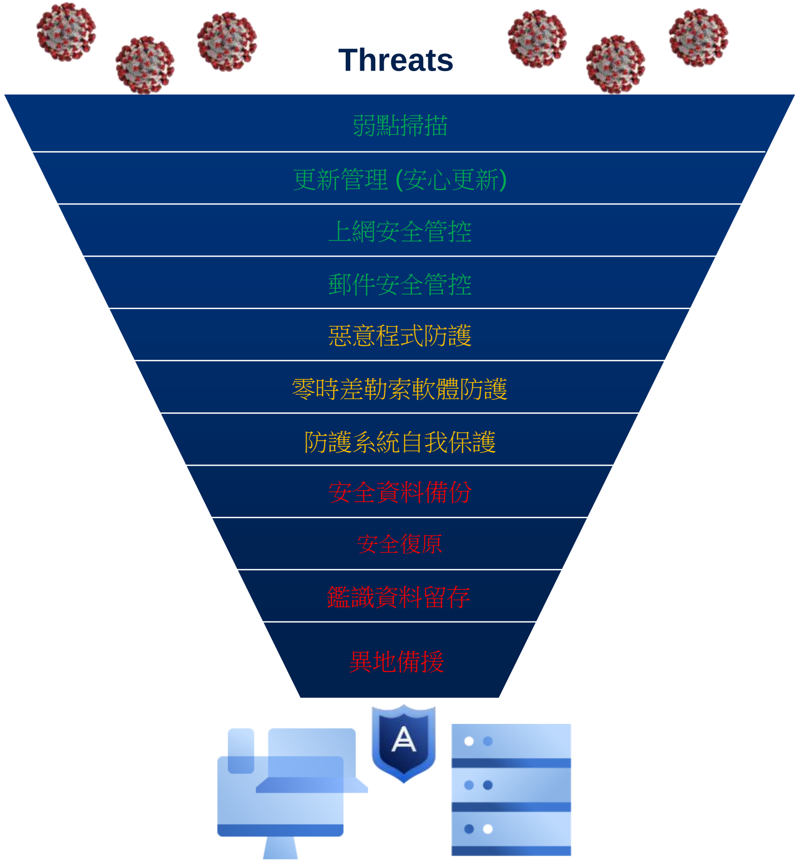
augmented with AI and ML technology, will continue to evolve to address increasingly sophisticated attacks. While preventing these attacks is the goal, organizations must also have the tools for rapid, certain data recovery.

Acronis

雙總部
分別位於瑞士和新加

Acronis Cyber Protect Cloud 超融合多層次防護

- 事前預防
  - 資安情資及防護建議
  - 弱點掃描
  - 更新管理 (安心更新)
  - 上網安全管控
  - 郵件安全管控
  - 週邊裝置管控 (資料外洩管控)
- 事中防護
  - 惡意程式防護
  - 零時差勒索軟體防護
  - 防護系統自我保護
- 事後回復
  - 資料備份 / 連續資料備份
  - 快速資料復原
  - 安全復原 / 備份檔掃毒
  - 遠端資料抹除
  - 資安鑑識資料留存
  - 異地備援



智能資安情資整合防護 自動提供防護計畫

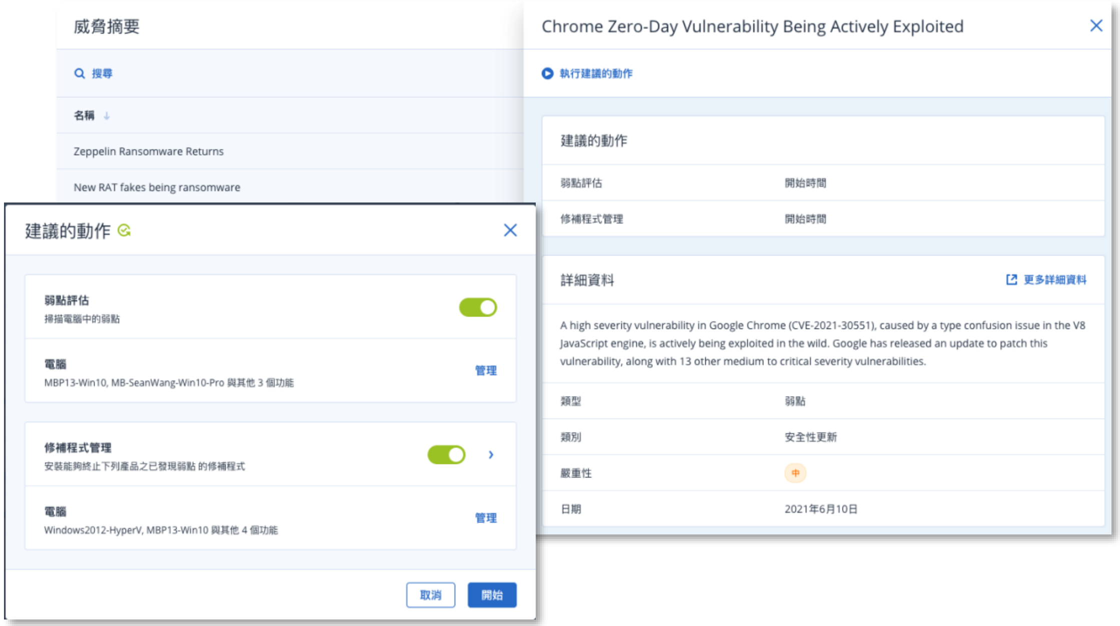
Unique

使用來自 Acronis CPOC 的情資 降低最新威脅造成的風險

Acronis CPOC 會監控網路安全態勢並發佈威脅警示。Acronis 產品會自動根據這些安全性警示提供防護計畫。這種方法會導致備份更為頻繁、更深入的 AV 掃描、安裝特定的修補程式等，從而提供更佳防護。

保護計畫將在情況恢復正常時復原。

- 最快之方式減少惡意軟體傳播、自然災害等造成的業務停機時間
- 減少反應時間
- 避免資料遺失



威脅摘要

搜尋

名稱 ↓
Zeppelin Ransomware Returns
New RAT fakes being ransomware

建議的動作

弱點評估 ●
掃描電腦中的弱點

電腦 管理
MBP13-Win10, MB-SeanWang-Win10-Pro 與其他 3 個功能

修補程式管理 ● ›
安裝能夠終止下列產品之已發現弱點 的修補程式

電腦 管理
Windows2012-HyperV, MBP13-Win10 與其他 4 個功能

取消 開始

Chrome Zero-Day Vulnerability Being Actively Exploited

執行建議的動作

建議的動作

弱點評估	開始時間
修補程式管理	開始時間

詳細資料 更多詳細資料

A high severity vulnerability in Google Chrome (CVE-2021-30551), caused by a type confusion issue in the V8 JavaScript engine, is actively being exploited in the wild. Google has released an update to patch this vulnerability, along with 13 other medium to critical severity vulnerabilities.

類型	弱點
類別	安全性更新
嚴重性	中
日期	2021年6月10日

為什麼？ 反應時間更快，以及防止停機和資料遺失

安心更新

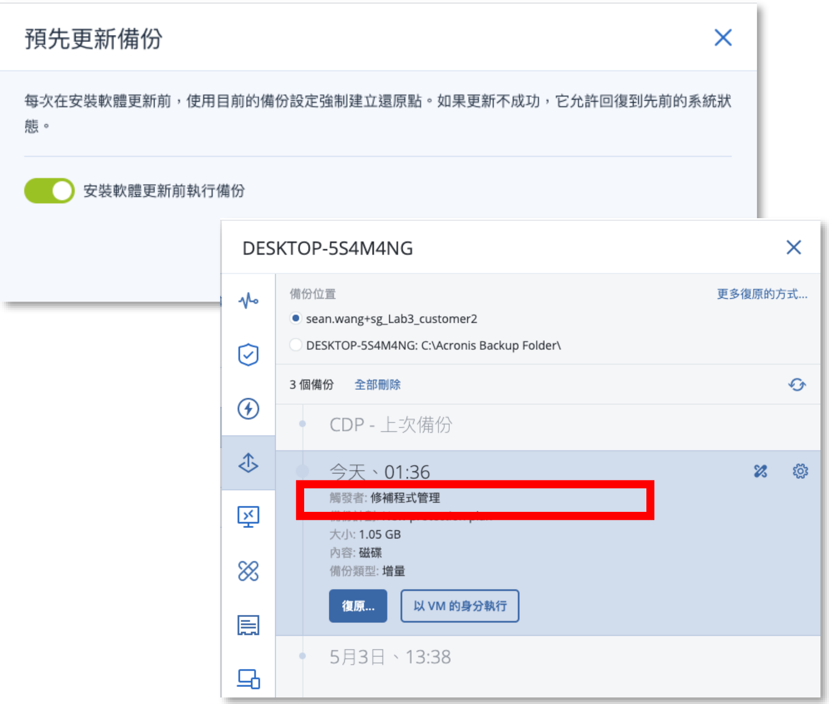
Unique

於修補前備份端點， 以快速回復至運作狀態

有問題的系統修補程式會導致系統不安全，但修補程式管理回復存在一定的局限性，會很慢。

防故障修補會先建立所選電腦的映像備份，再安裝系統或應用程式修補程式以便快速回復。

- 完整映像備份是回復至可用狀態的最快最簡單的方法



預先更新備份

每次在安裝軟體更新前，使用目前的備份設定強制建立還原點。如果更新不成功，它允許回復到先前的系統狀態。

安裝軟體更新前執行備份

DESKTOP-5S4M4NG

備份位置

● sean.wang+sg_Lab3_customer2

○ DESKTOP-5S4M4NG: C:\Acronis Backup Folder\

3 個備份

CDP - 上次備份

今天、01:36

觸發者: 修補程式管理

大小: 1.05 GB

內容: 磁碟

備份類型: 增量

5月3日、13:38

為什麼？ 節省資源，同時支援更快更為可靠的作業

AI 智能零時差勒索軟體防護

Unique

適用於 Windows、Linux 和 macOS 的惡意軟體防護

- 勒索軟體偵測和資料復原
- 挖礦程序偵測
- 即時防護和隨需掃描
- 自我防護：保護 Acronis 元件 (如登錄、服務停止、Acronis 檔案保護)
- Acronis Active Protection 會不斷觀察電腦上資料檔案的變動狀況。一組行為是正常且為預期中的情況。另一組行為可能會發出訊號，通知有可疑的動作正在對檔案進行敵對行動。Acronis 的方法會注視這些行動，並將其與惡意行為模式進行比較。這種方法在識別勒索病毒攻擊方面，非常強而有力，即便是來自從未被發現的勒索病毒變種，亦無法閃避。

安心復原

Unique

將 AV 更新和修補程式管理整合至復原程序 避免重複感染

備份中的作業系統映像或應用程式可能含有讓使用者處於風險中的弱點。

修補電腦並套用最新的反惡意軟體定義檔，可讓使用者還原套用最新修補程式的作業系統映像，避免重覆感染。

- 更新病毒碼資料庫
- 安裝最新的安全性修補程式

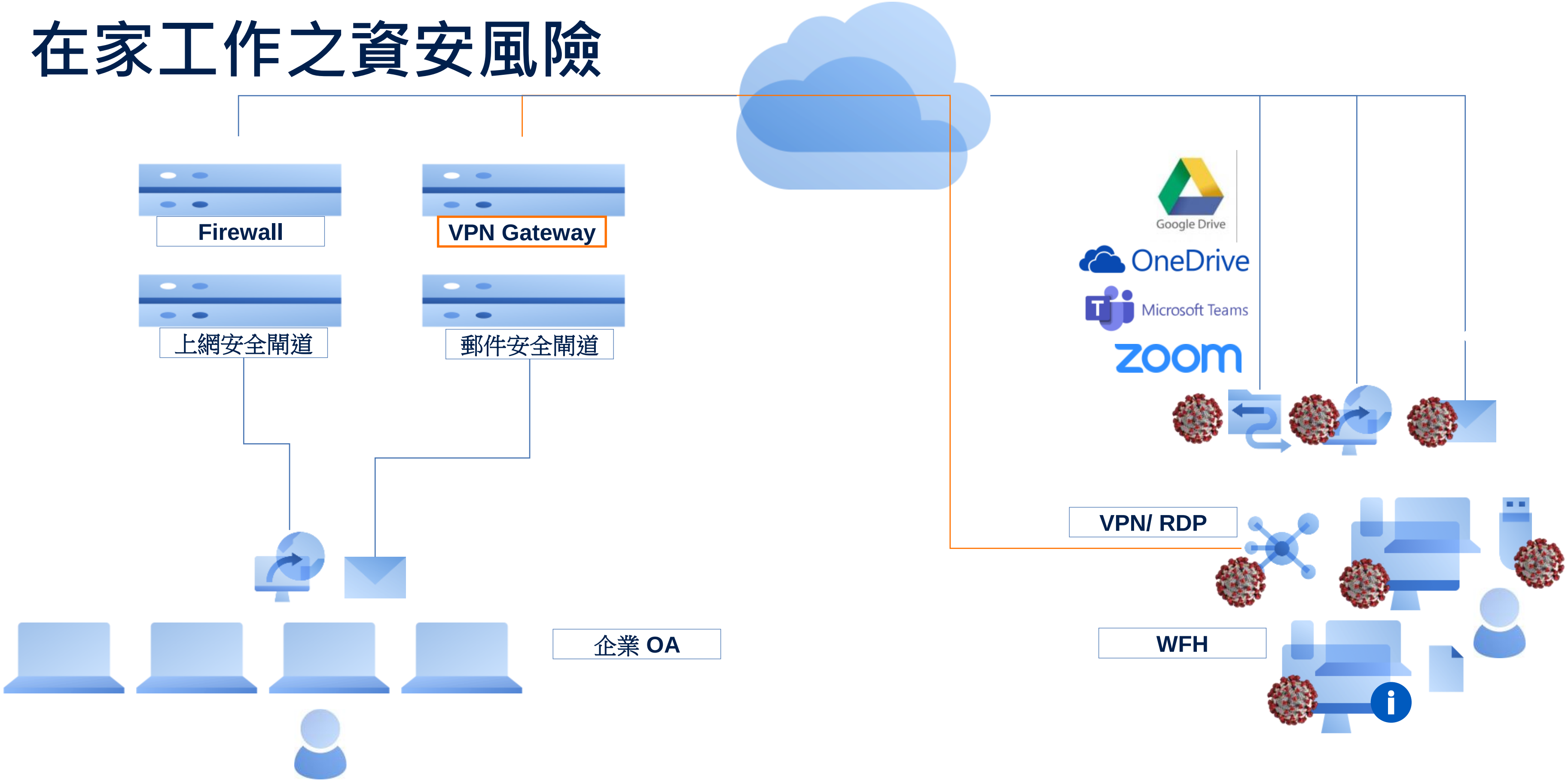
為什麼？節省時間、精力和資料。使用受感染/有弱點的映像快速復原，無需額外步驟

Acronis

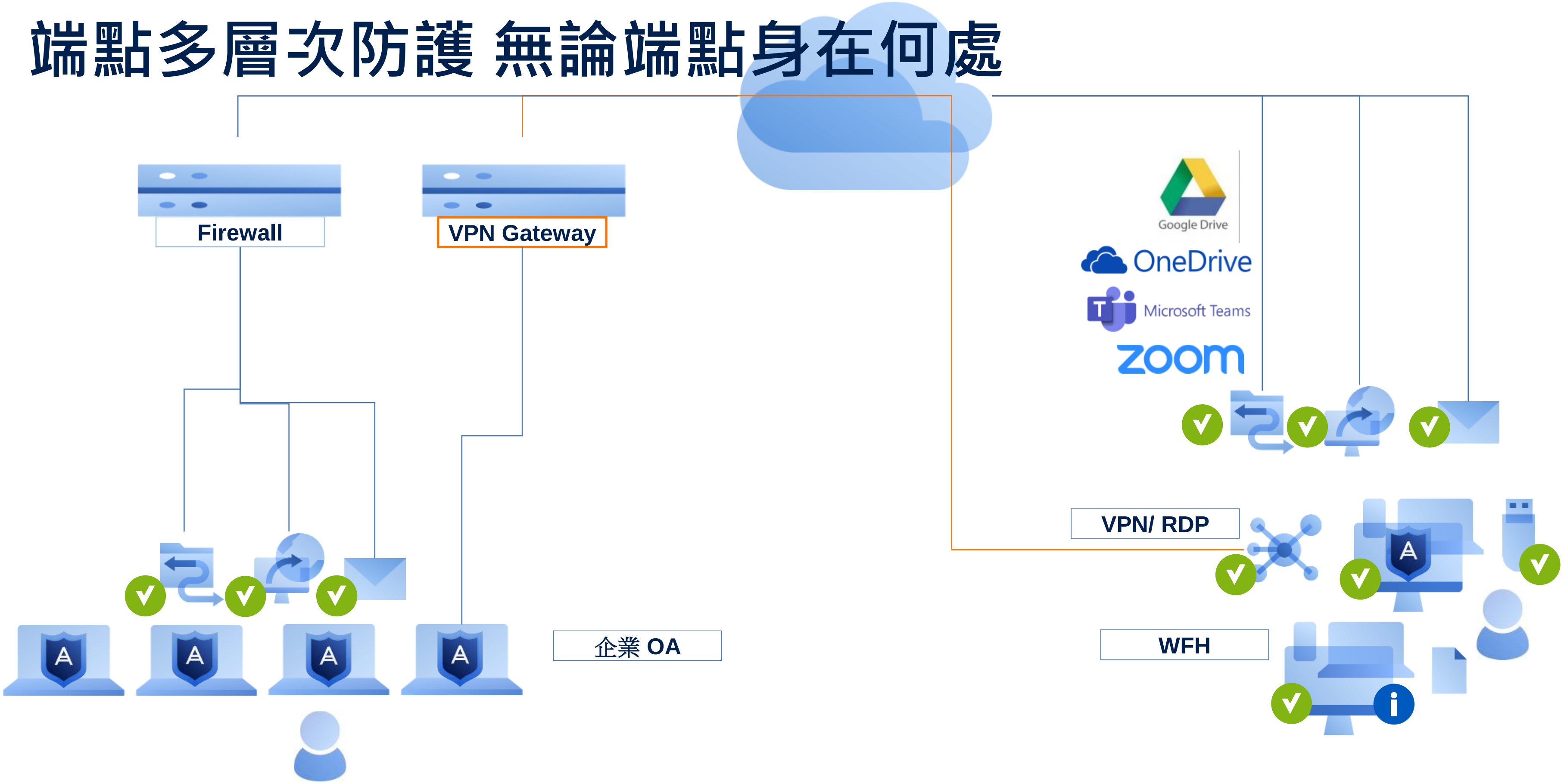
#CyberFit

居家/ 遠距連線工作安全管控

在家工作之資安風險


Firewall
VPN Gateway
上網安全閘道
郵件安全閘道
企業 OA
Google Drive
OneDrive
Microsoft Teams
zoom
VPN/ RDP
WFH

端點多層次防護 無論端點身在何處



Acronis

#CyberFit

自動進化之超融合多層次防護

融合為一的力量

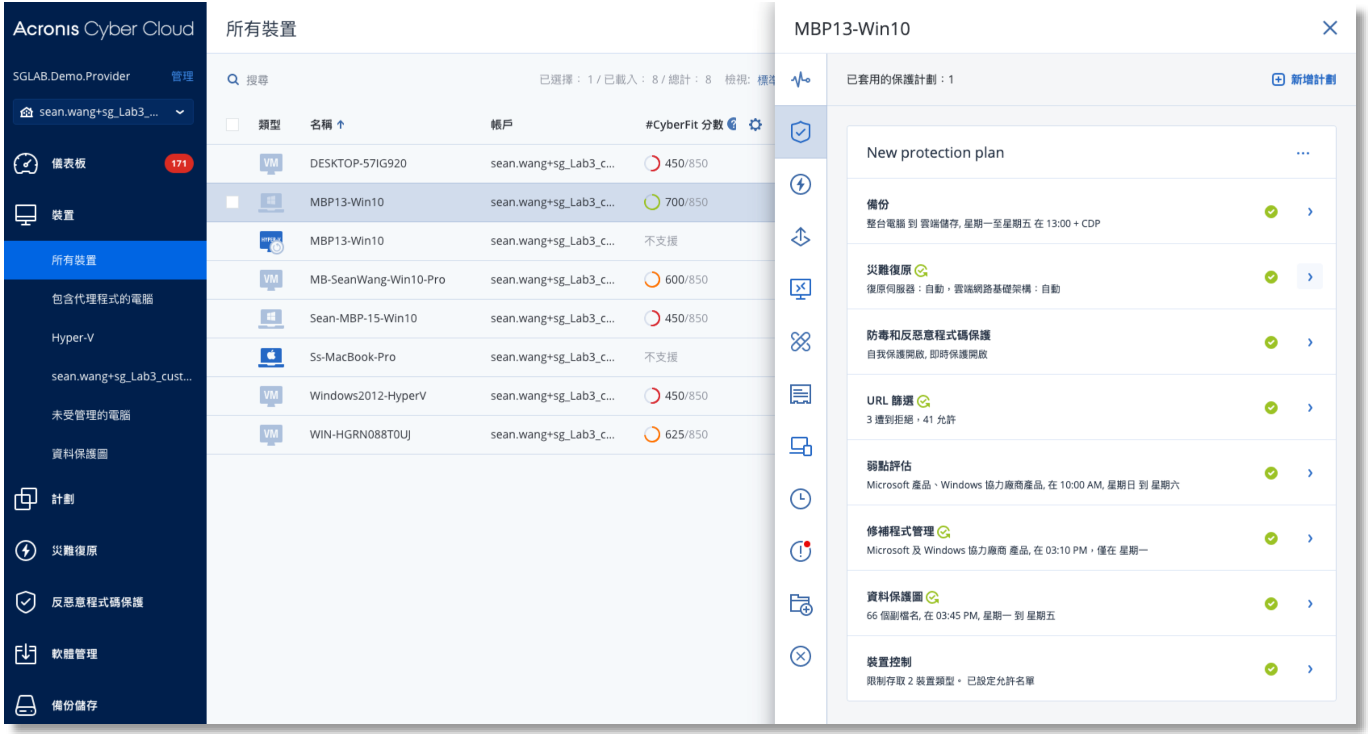
Unique

在所有層面進行整合：介面、管理、產品、技術

- ✓ 單一代理程式
- ✓ 單一管理控制台
- ✓ 單一防護政策
- ✓ 單一後端
- ✓ 單一使用者介面
- ✓ 單一授權
- ✓ 單一廠商支援專線

利用「融合為一」的強大功能，可以：

- 化繁為簡
- 降低成本



Acronis Cyber Cloud

SGLAB.Demo.Provider 管理

sean.wang+sg_Lab3_...

- 儀表板 171
- 裝置
  - 所有裝置
  - 包含代理程式的電腦
  - Hyper-V
  - sean.wang+sg_Lab3_cust...
  - 未受管理的電腦
  - 資料保護圖
- 計劃
- 災難復原
- 反惡意程式碼保護
- 軟體管理
- 備份儲存

所有裝置

搜尋　　已選擇：1 / 已載入：8 / 總計：8　檢視：標準

類型	名稱 ↑	帳戶	#CyberFit 分數
VM	DESKTOP-57IG920	sean.wang+sg_Lab3_c...	450/850
	MBP13-Win10	sean.wang+sg_Lab3_c...	700/850
HYPER-V	MBP13-Win10	sean.wang+sg_Lab3_c...	不支援
VM	MB-SeanWang-Win10-Pro	sean.wang+sg_Lab3_c...	600/850
	Sean-MBP-15-Win10	sean.wang+sg_Lab3_c...	450/850
	Ss-MacBook-Pro	sean.wang+sg_Lab3_c...	不支援
VM	Windows2012-HyperV	sean.wang+sg_Lab3_c...	450/850
VM	WIN-HGRN088T0UJ	sean.wang+sg_Lab3_c...	625/850

MBP13-Win10 ✕

已套用的保護計劃：1　　新增計劃

New protection plan ...

備份 ✓
整台電腦 到 雲端儲存, 星期一至星期五 在 13:00 + CDP

災難復原 ✓
復原伺服器：自動，雲端網路基礎架構：自動

防毒和反惡意程式碼保護 ✓
自我保護開啟, 即時保護開啟

URL 篩選 ✓
3 遭到拒絕，41 允許

弱點評估 ✓
Microsoft 產品、Windows 協力廠商產品, 在 10:00 AM, 星期日 到 星期六

修補程式管理 ✓
Microsoft 及 Windows 協力廠商 產品, 在 03:10 PM，僅在 星期一

資料保護圖 ✓
66 個副檔名, 在 03:45 PM, 星期一 到 星期五

裝置控制 ✓
限制存取 2 裝置類型。 已設定允許名單

備份已經成為勒索病毒的目標

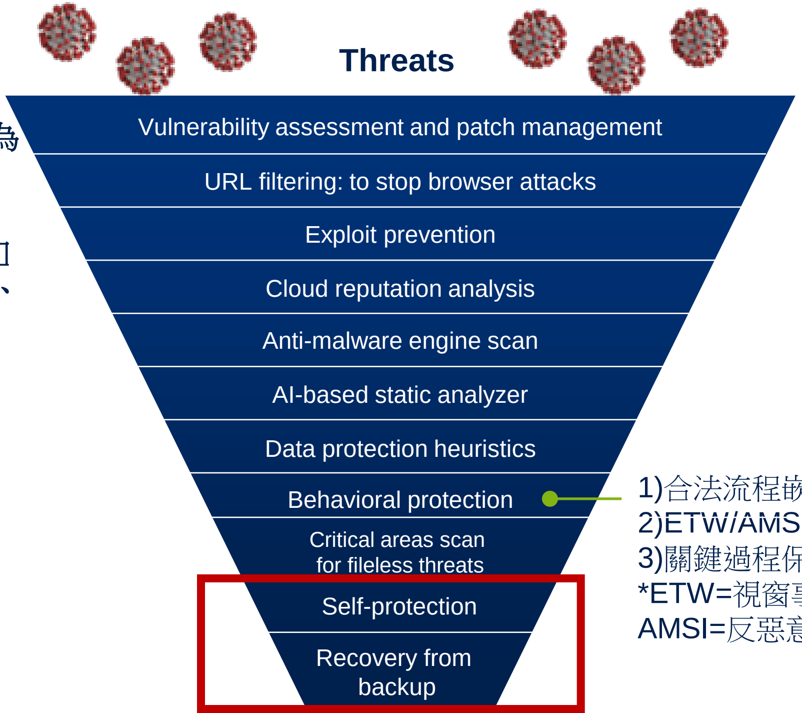
- 為了達到勒索目的,網路犯罪者知道企業會以備份來復原,因此攻擊備份成為目標
- 雲備份,已經擋不住所謂的勒索病毒的攻擊;他可以透過阻斷連結,或是,侵入端點的備份代理, 輕易取得進入雲備份的訊息！
- 只是用321法則,已經不夠了！
- 需要用新型態資安保護架構, 去防禦和回復勒索病毒攻擊。

Acronis在備份和底層 I/O 方面的專業知識,在行為偵測技術方面具有優勢

新的惡意軟體技術，例如RIPlace使用符號連結加密檔，躲避了微軟、賽門鐵克、索福斯、邁克菲、crowdstrike、Malwarebytes 掃描器的發現

Acronis 可防止惡意軟體使用底層數據的躲避技術

代理和備份自我保護：自動恢復為最後一層保護



1)合法流程嵌入式檢測
2)ETW/AMSI 事件分析*
3)關鍵過程保護
*ETW=視窗事件追蹤，
AMSI=反惡意軟體掃描介面

Acronis 資安防護功能 獲業界認可

Microsoft

病毒計畫 (MVI) 成員

VIRUSTOTAL 成員

CSA cloud security alliance℠

Cloud Security Alliance 成員

MEMBER amtso Anti-Malware Testing Standards Organization

Anti-Malware Testing Standard Organization 成員

APWG

Anti-Phishing Working Group 成員

MRG-Effitas 參與者和測試獲勝者

AM ANTI-MALWARE

Anti-Malware Test Lab 參與者和測試獲勝者

ICSA labs CERTIFIED ANTI-MALWARE ENDPOINT PRODUCT | FOR BUSINESS Certified Since July 2020

ICSA Labs 認證

NioGuard Security Lab

NioGuard Security Lab 參與者和測試獲勝者

AV comparatives APPROVED Business Security JUL 2020

AV-Comparatives 認可的商業安全性產品

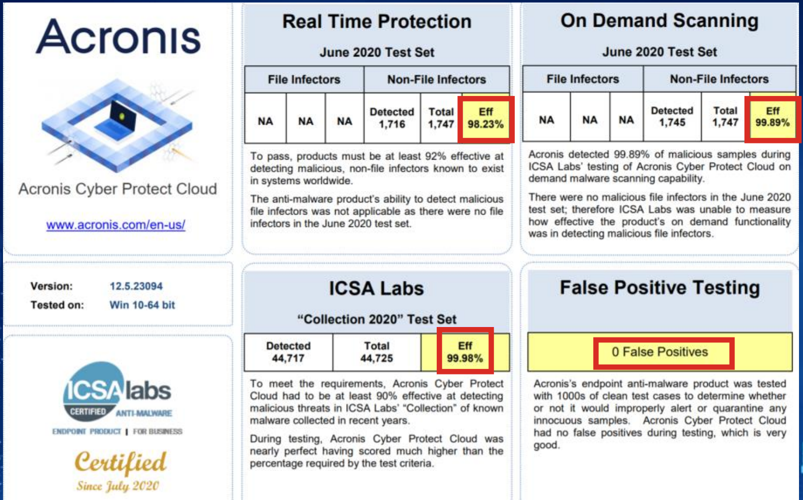
Passed VIRUS 100

VB100 認證

AV TEST

AV-Test 參與者和測試獲勝者

無數業界資安測試認證



Acronis

Acronis Cyber Protect Cloud

www.acronis.com/en-us/

Version: 12.5.23094
Tested on: Win 10-64 bit

ICSA labs CERTIFIED ANTI-MALWARE
ENDPOINT PRODUCT | FOR BUSINESS
Certified
Since July 2020

Real Time Protection

June 2020 Test Set

File Infectors			Non-File Infectors		
NA	NA	NA	Detected 1,716	Total 1,747	Eff 98.23%

To pass, products must be at least 92% effective at detecting malicious, non-file infectors known to exist in systems worldwide.

The anti-malware product's ability to detect malicious file infectors was not applicable as there were no file infectors in the June 2020 test set.

On Demand Scanning

June 2020 Test Set

File Infectors			Non-File Infectors		
NA	NA	NA	Detected 1,745	Total 1,747	Eff 99.89%

Acronis detected 99.89% of malicious samples during ICSA Labs' testing of Acronis Cyber Protect Cloud on demand malware scanning capability.

There were no malicious file infectors in the June 2020 test set; therefore ICSA Labs was unable to measure how effective the product's on demand functionality was in detecting malicious file infectors.

ICSA Labs

"Collection 2020" Test Set

Detected	Total	Eff
44,717	44,725	99.98%

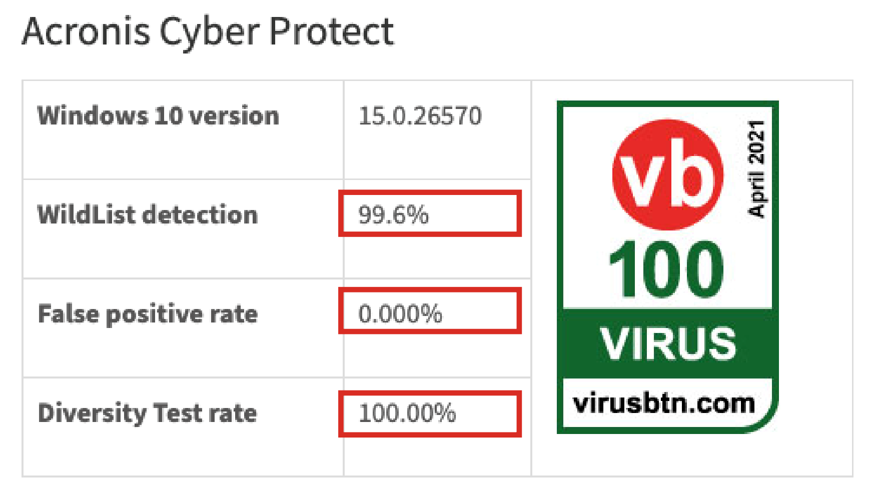
To meet the requirements, Acronis Cyber Protect Cloud had to be at least 90% effective at detecting malicious threats in ICSA Labs' "Collection" of known malware collected in recent years.

During testing, Acronis Cyber Protect Cloud was nearly perfect having scored much higher than the percentage required by the test criteria.

False Positive Testing

0 False Positives

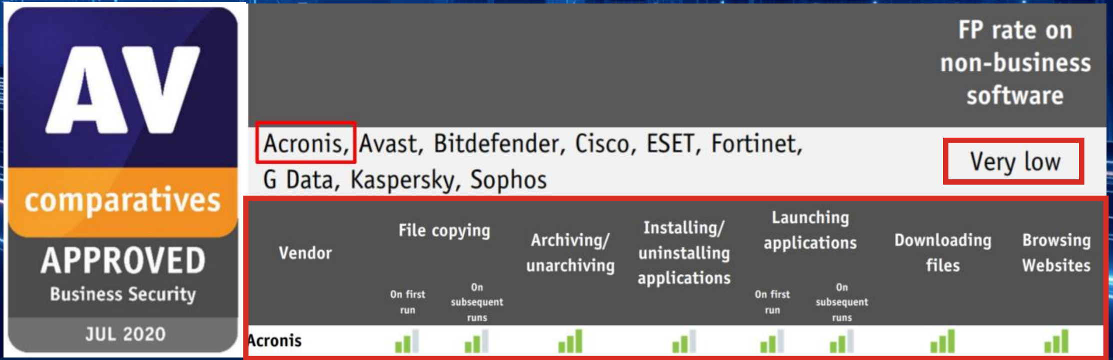
Acronis's endpoint anti-malware product was tested with 1000s of clean test cases to determine whether or not it would improperly alert or quarantine any innocuous samples. Acronis Cyber Protect Cloud had no false positives during testing, which is very good.



Acronis Cyber Protect

Windows 10 version	15.0.26570
WildList detection	99.6%
False positive rate	0.000%
Diversity Test rate	100.00%

vb 100 VIRUS April 2021 virusbtn.com

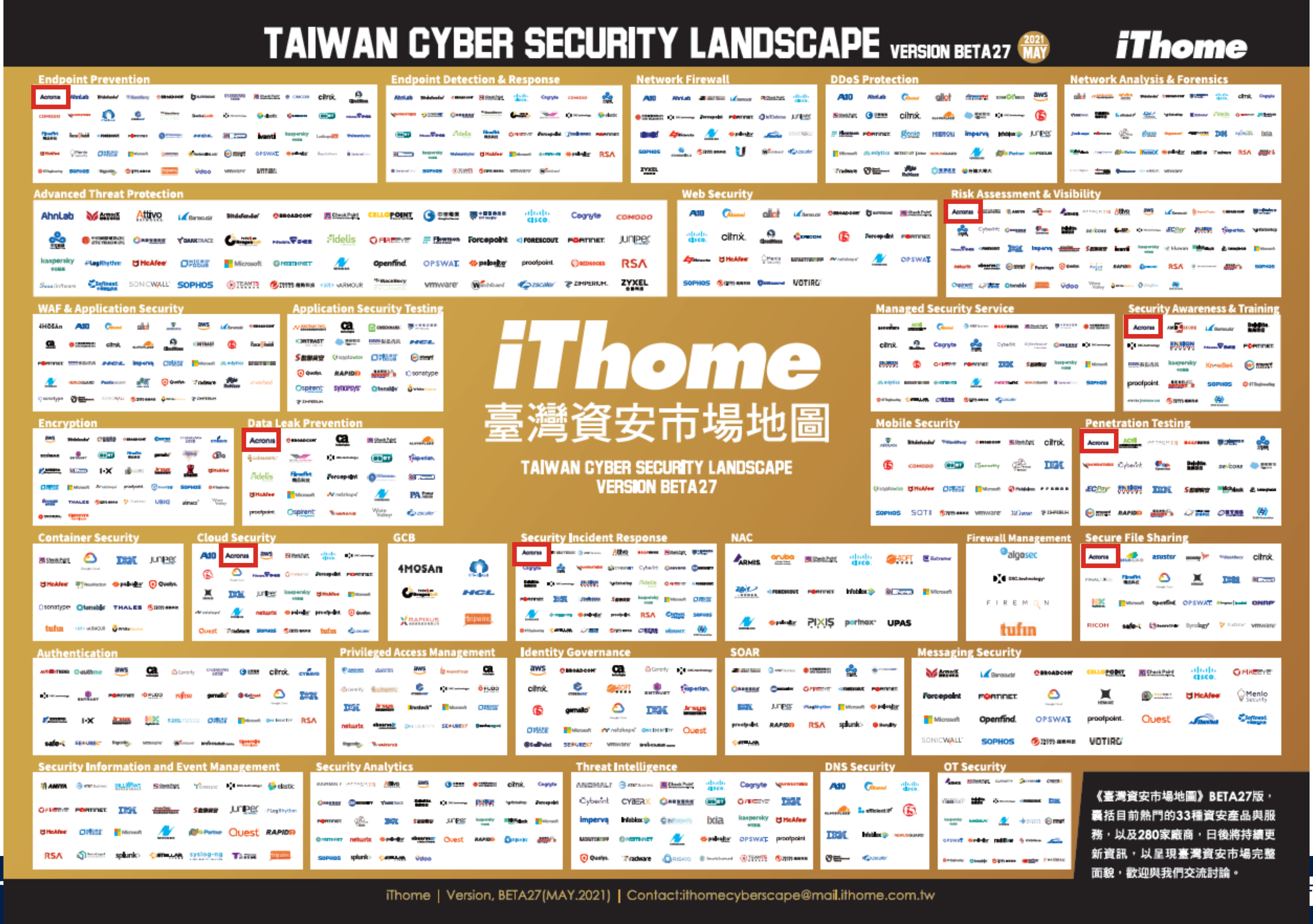


AV comparatives APPROVED Business Security JUL 2020

	FP rate on non-business software
Acronis, Avast, Bitdefender, Cisco, ESET, Fortinet, G Data, Kaspersky, Sophos	Very low

Vendor	File copying		Archiving/ unarchiving	Installing/ uninstalling applications	Launching applications		Downloading files	Browsing Websites
	On first run	On subsequent runs			On first run	On subsequent runs		
Acronis	▮	▮	▮	▮	▮	▮	▮	▮

- ✓ 最高偵測率
- ✓ 零誤判率
- ✓ 最佳效能



TAIWAN CYBER SECURITY LANDSCAPE VERSION BETA27 2021 MAY

iThome

Endpoint Prevention

Endpoint Detection & Response

Network Firewall

DDoS Protection

Network Analysis & Forensics

Advanced Threat Protection

Web Security

Risk Assessment & Visibility

WAF & Application Security

Application Security Testing

Managed Security Service

Security Awareness & Training

Encryption

Data Leak Prevention

Mobile Security

Penetration Testing

Container Security

Cloud Security

GCB

Security Incident Response

NAC

Firewall Management

Secure File Sharing

Authentication

Privileged Access Management

Identity Governance

SOAR

Messaging Security

Security Information and Event Management

Security Analytics

Threat Intelligence

DNS Security

OT Security

iThome

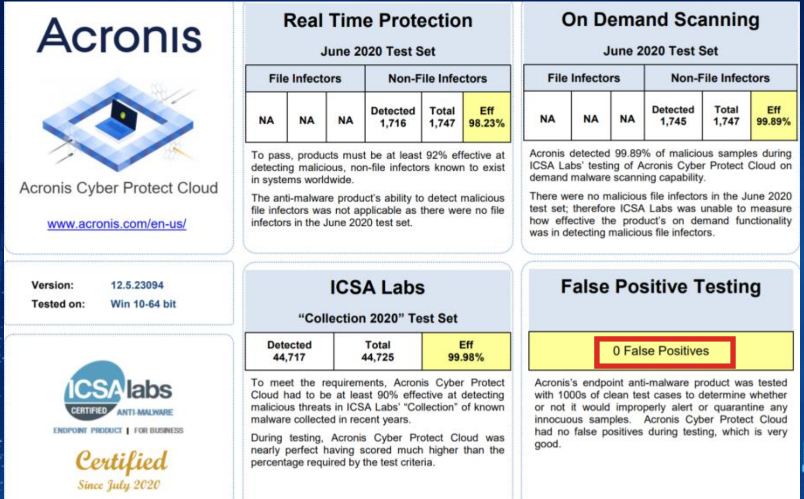
臺灣資安市場地圖

TAIWAN CYBER SECURITY LANDSCAPE
VERSION BETA27

《臺灣資安市場地圖》BETA27版，囊括目前熱門的33種資安產品與服務，以及280家廠商，日後將持續更新資訊，以呈現臺灣資安市場完整面貌，歡迎與我們交流討論。

iThome | Version, BETA27(MAY.2021) | Contact:ithomecyberscape@mail.ithome.com.tw

無數業界資安測試認證



Acronis

Acronis Cyber Protect Cloud

www.acronis.com/en-us/

Version:	12.5.23094
Tested on:	Win 10-64 bit

ICSA labs CERTIFIED ANTI-MALWARE ENDPOINT PRODUCT | FOR BUSINESS Certified Since July 2020

Real Time Protection

June 2020 Test Set

File Infectors			Non-File Infectors		
NA	NA	NA	Detected 1,716	Total 1,747	Eff 98.23%

To pass, products must be at least 92% effective at detecting malicious, non-file infectors known to exist in systems worldwide.

The anti-malware product's ability to detect malicious file infectors was not applicable as there were no file infectors in the June 2020 test set.

On Demand Scanning

June 2020 Test Set

File Infectors			Non-File Infectors		
NA	NA	NA	Detected 1,745	Total 1,747	Eff 99.89%

Acronis detected 99.89% of malicious samples during ICSA Labs' testing of Acronis Cyber Protect Cloud on demand malware scanning capability.

There were no malicious file infectors in the June 2020 test set; therefore ICSA Labs was unable to measure how effective the product's on demand functionality was in detecting malicious file infectors.

ICSA Labs

"Collection 2020" Test Set

Detected	Total	Eff
44,717	44,725	99.98%

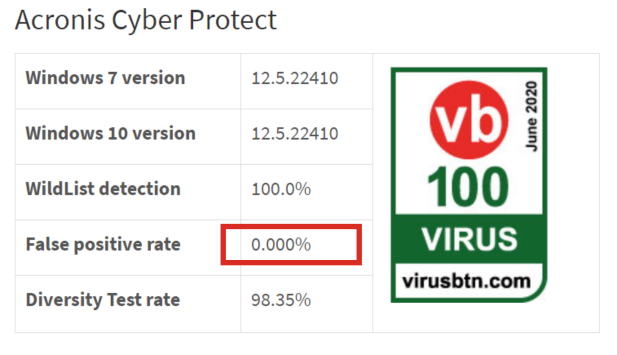
To meet the requirements, Acronis Cyber Protect Cloud had to be at least 90% effective at detecting malicious threats in ICSA Labs' "Collection" of known malware collected in recent years.

During testing, Acronis Cyber Protect Cloud was nearly perfect having scored much higher than the percentage required by the test criteria.

False Positive Testing

0 False Positives

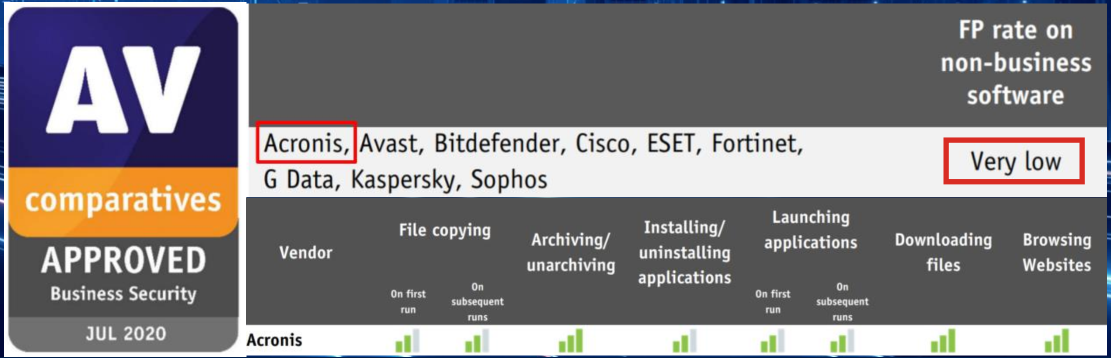
Acronis's endpoint anti-malware product was tested with 1000s of clean test cases to determine whether or not it would improperly alert or quarantine any innocuous samples. Acronis Cyber Protect Cloud had no false positives during testing, which is very good.



Acronis Cyber Protect

Windows 7 version	12.5.22410
Windows 10 version	12.5.22410
WildList detection	100.0%
False positive rate	0.000%
Diversity Test rate	98.35%

vb 100 VIRUS June 2020 virusbtn.com



AV comparatives APPROVED Business Security JUL 2020

	FP rate on non-business software
Acronis, Avast, Bitdefender, Cisco, ESET, Fortinet, G Data, Kaspersky, Sophos	Very low

Vendor	File copying		Archiving/ unarchiving	Installing/ uninstalling applications	Launching applications		Downloading files	Browsing Websites
	On first run	On subsequent runs			On first run	On subsequent runs		
Acronis	▂▄▆	▂▄▆	▂▄▆	▂▄▆	▂▄▆	▂▄▆	▂▄▆	▂▄▆

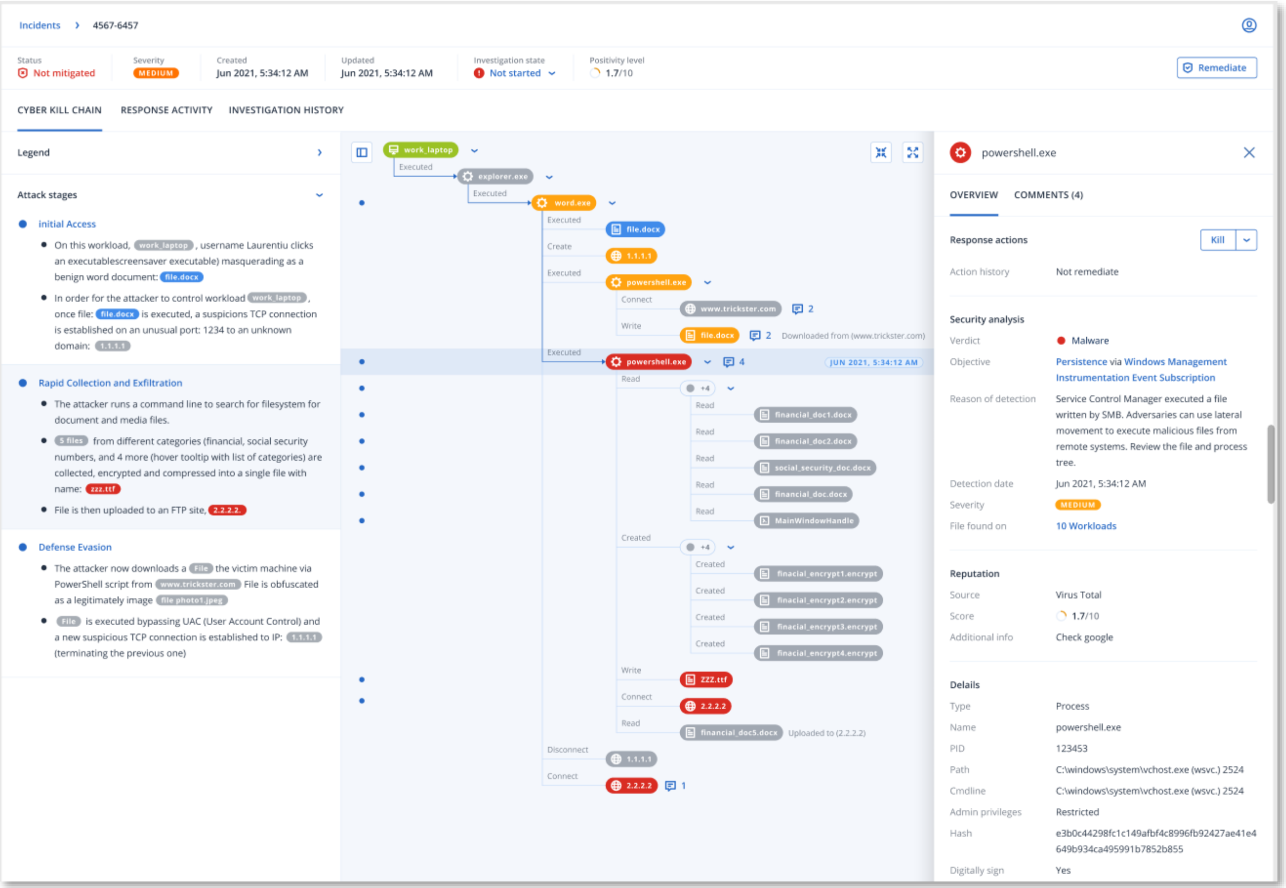
Acronis

#CyberFit

Acronis Advanced Security + EDR

Visibility

- Visibility in attack steps:
  - How it got in?
  - How did it hide its tracks?
  - What did it harm?
  - How did it spread?
- System activities
  - Create process
  - Create/ Move/ Rename file
  - Set registry value
  - Network Activities
    - C&C



Incidents › 4567-6457

Status	Severity	Created	Updated	Investigation state	Positivity level
Not mitigated	MEDIUM	Jun 2021, 5:34:12 AM	Jun 2021, 5:34:12 AM	Not started	1.7/10

Remediate

CYBER KILL CHAIN | RESPONSE ACTIVITY | INVESTIGATION HISTORY

Legend

Attack stages

- initial Access
  - On this workload, work_laptop , username Laurentiu clicks an executablescreensaver executable) masquerading as a benign word document: file.docx
  - In order for the attacker to control workload work_laptop , once file: file.docx is executed, a suspicions TCP connection is established on an unusual port: 1234 to an unknown domain: 1.1.1.1
- Rapid Collection and Exfiltration
  - The attacker runs a command line to search for filesystem for document and media files.
  - 5 files from different categories (financial, social security numbers, and 4 more (hover tooltip with list of categories) are collected, encrypted and compressed into a single file with name: zzz.ttf
  - File is then uploaded to an FTP site, 2.2.2.2.
- Defense Evasion
  - The attacker now downloads a File the victim machine via PowerShell script from www.trickster.com File is obfuscated as a legitimately image file photo1.jpeg
  - File is executed bypassing UAC (User Account Control) and a new suspicious TCP connection is established to IP: 1.1.1.1 (terminating the previous one)

powershell.exe

OVERVIEW | COMMENTS (4)

Response actions — Kill

Action history	Not remediate

Security analysis

Verdict	Malware
Objective	Persistence via Windows Management Instrumentation Event Subscription
Reason of detection	Service Control Manager executed a file written by SMB. Adversaries can use lateral movement to execute malicious files from remote systems. Review the file and process tree.
Detection date	Jun 2021, 5:34:12 AM
Severity	MEDIUM
File found on	10 Workloads

Reputation

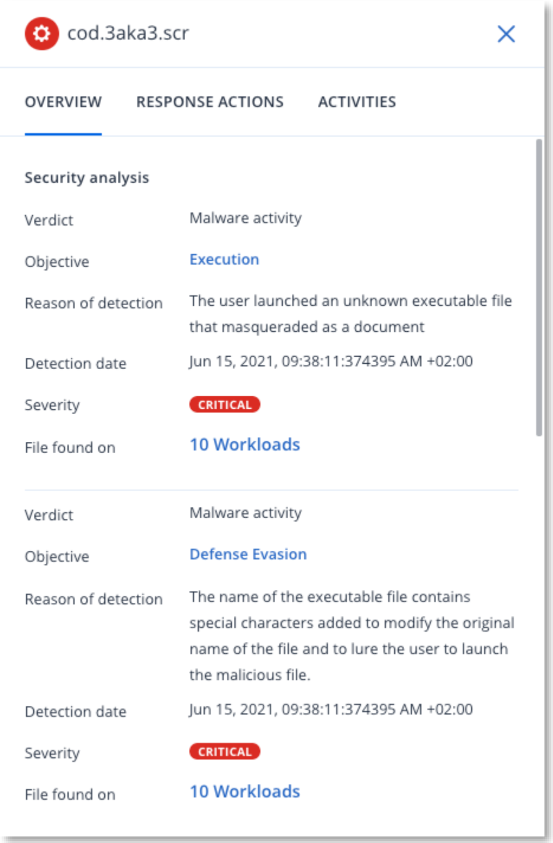
Source	Virus Total
Score	1.7/10
Additional info	Check google

Details

Type	Process
Name	powershell.exe
PID	123453
Path	C:\windows\system\vchost.exe (wsvc.) 2524
Cmdline	C:\windows\system\vchost.exe (wsvc.) 2524
Admin privileges	Restricted
Hash	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Digitally sign	Yes

Analyze

- Interpreted attack
  - Objective – MITRE ATT&CK
  - Reason of detection
- Attack Stages
  - Chronological view
  - Story Line for incident investigation

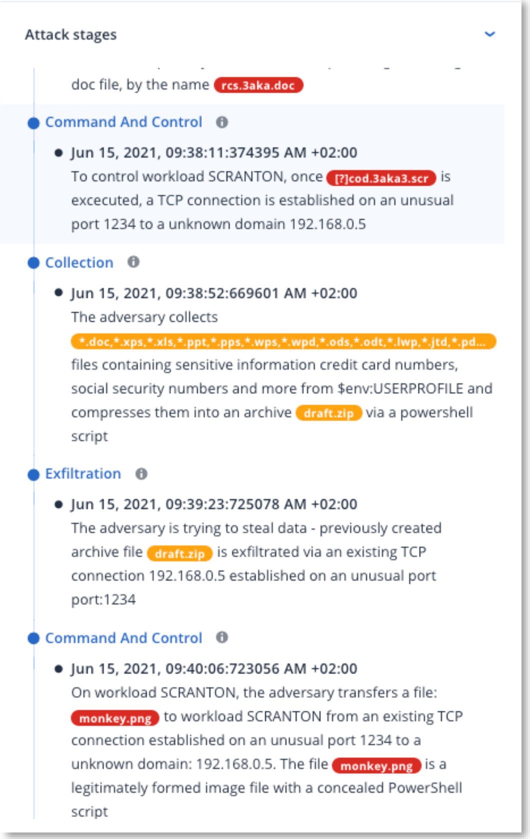


cod.3aka3.scr

Security analysis

Verdict	Malware activity
Objective	Execution
Reason of detection	The user launched an unknown executable file that masqueraded as a document
Detection date	Jun 15, 2021, 09:38:11:374395 AM +02:00
Severity	CRITICAL
File found on	10 Workloads

Verdict	Malware activity
Objective	Defense Evasion
Reason of detection	The name of the executable file contains special characters added to modify the original name of the file and to lure the user to launch the malicious file.
Detection date	Jun 15, 2021, 09:38:11:374395 AM +02:00
Severity	CRITICAL
File found on	10 Workloads



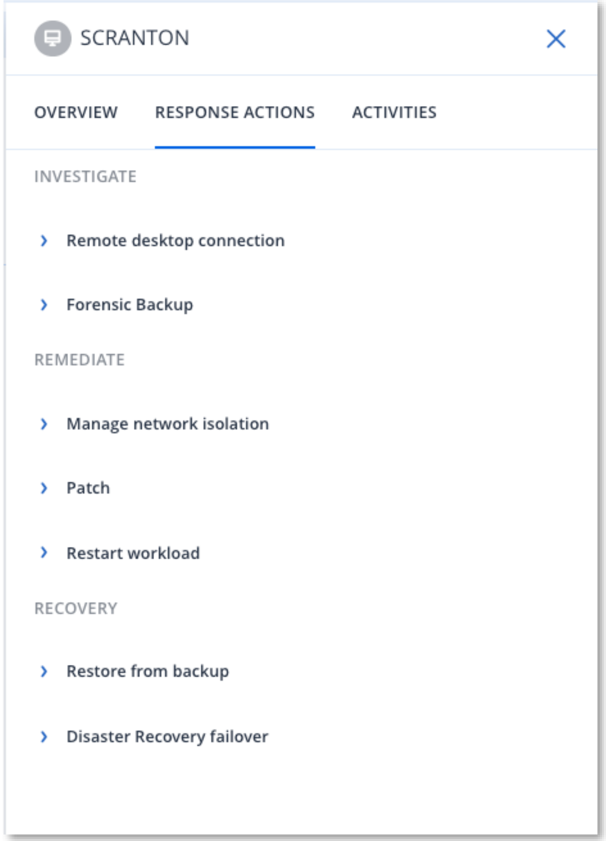
Attack stages

doc file, by the name rcs.3aka.doc

- Command And Control
  - Jun 15, 2021, 09:38:11:374395 AM +02:00
    To control workload SCRANTON, once [?]cod.3aka3.scr is excecuted, a TCP connection is established on an unusual port 1234 to a unknown domain 192.168.0.5
- Collection
  - Jun 15, 2021, 09:38:52:669601 AM +02:00
    The adversary collects *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pd... files containing sensitive information credit card numbers, social security numbers and more from $env:USERPROFILE and compresses them into an archive draft.zip via a powershell script
- Exfiltration
  - Jun 15, 2021, 09:39:23:725078 AM +02:00
    The adversary is trying to steal data - previously created archive file draft.zip is exfiltrated via an existing TCP connection 192.168.0.5 established on an unusual port port:1234
- Command And Control
  - Jun 15, 2021, 09:40:06:723056 AM +02:00
    On workload SCRANTON, the adversary transfers a file: monkey.png to workload SCRANTON from an existing TCP connection established on an unusual port 1234 to a unknown domain: 192.168.0.5. The file monkey.png is a legitimately formed image file with a concealed PowerShell script

Reponse to dangerous computer

- Investigate
  - Remote desktop connection
  - Forensic Backup
- Remediate
  - Isolation
  - Patch
  - Restart workload
- Recovery
  - Restore from backup
  - Disaster Recovery Failover



SCRANTON

OVERVIEW RESPONSE ACTIONS ACTIVITIES

INVESTIGATE

› Remote desktop connection

› Forensic Backup

REMEDIATE

› Manage network isolation

› Patch

› Restart workload

RECOVERY

› Restore from backup

› Disaster Recovery failover

Acronis Advanced Security + EDR

Detect – Full Visibility

- Enables you to see beyond standard events in their workloads
  - Attack chain – Story Line complete visibility
  - Data being targeted and/or exfiltrated
  - Recommended actions to all points of an attack

Analyze – Interpreted attack

- Narrate the incidents in human language sentences emphasizing the objectives of each step and artefacts target by the attacker
  - eliminated the need to build or buy SOC services
  - Easy to understand
  - MITRE ATT&CK framework

Respond – Multiple ways

- **Investigate** with actions like remote control
- **Remediate** with actions like:
  - Quarantine workload, kill malware processes, rollback registry, etc.
- **Recover** with Acronis Backup and Disaster Recovery
- **Prevent** with patch software and block executing already analyzed threats

Acronis

#CyberFit

Protect Microsoft 365 with Acronis Cyber Protect Cloud

Easy, efficient, and secure Microsoft 365 backup

雙總部
分别位於瑞士和新加坡

輕鬆、高效、安全的 Microsoft 365 備份
讓客戶無憂無慮

無代理備份

簡化設定和維護的解決方案，無需在地端的安裝代理程式就可以在安全的Acronis Cloud執行.

在幾秒鐘內進行精細還原

在幾秒鐘內還原客戶所需的資料，如電子郵件、檔案、網站、連絡人、附件等。避免停機，並確保其業務連續性。

快速備份搜索

確保訪問客戶端備份的數據。在恢復之前，搜索特定的 Microsoft 365 項並立即使用它們。下載關鍵檔或附件，或從備份直接發送電子郵件。

完整 Microsoft 365 保護

Microsoft 365

Exchange

Backup for Microsoft Exchange Online

OneDrive

Backup for Microsoft OneDrive for Business

SharePoint

Backup for Microsoft SharePoint Online

Microsoft Teams

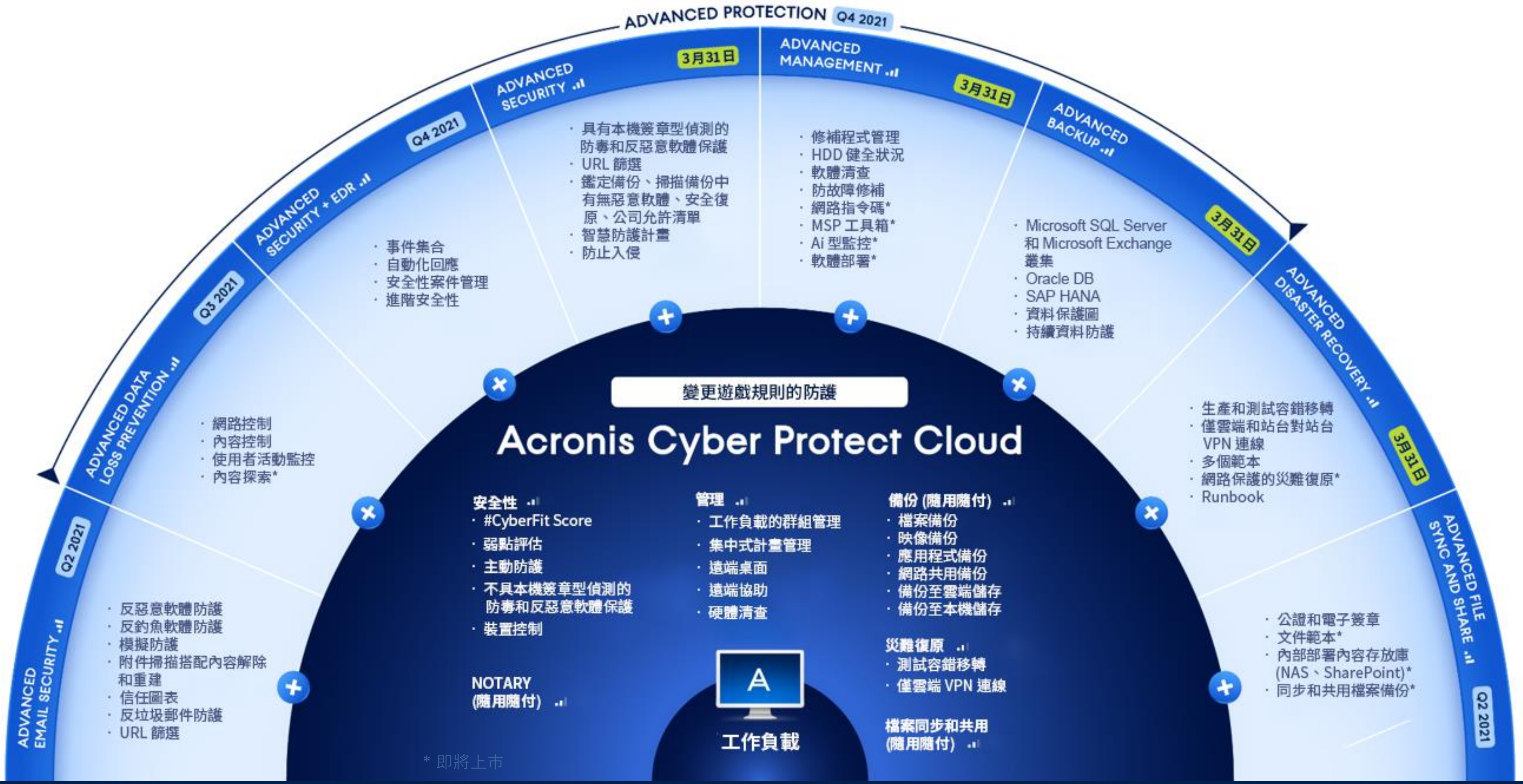
Backup for Microsoft Teams

Including call protection

- ✓ 從 Microsoft 資料中心直接備份到Acronis 雲端存儲
- ✓ 自動保護新的 Microsoft 365 使用者、群組和站台
- ✓ 通過Microsoft 365備份進行搜索，以便快速存取備份資料

New **無設限的個人微軟 365 郵箱備份到 Acronis 雲存儲**

Acronis 自動進化之超融合多層次防護



ADVANCED PROTECTION Q4 2021

ADVANCED EMAIL SECURITY Q2 2021

- 反惡意軟體防護
- 反釣魚軟體防護
- 模擬防護
- 附件掃描搭配內容解除和重建
- 信任圖表
- 反垃圾郵件防護
- URL 篩選

ADVANCED DATA LOSS PREVENTION Q3 2021

- 網路控制
- 內容控制
- 使用者活動監控
- 內容探索*

ADVANCED SECURITY + EDR Q4 2021

- 事件集合
- 自動化回應
- 安全性案件管理
- 進階安全性

ADVANCED SECURITY 3月31日

- 具有本機簽章型偵測的防毒和反惡意軟體保護
- URL 篩選
- 鑑定備份、掃描備份中有無惡意軟體、安全復原、公司允許清單
- 智慧防護計畫
- 防止入侵

ADVANCED MANAGEMENT 3月31日

- 修補程式管理
- HDD 健全狀況
- 軟體清查
- 防故障修補
- 網路指令碼*
- MSP 工具箱*
- Ai 型監控*
- 軟體部署*

ADVANCED BACKUP 3月31日

- Microsoft SQL Server 和 Microsoft Exchange 叢集
- Oracle DB
- SAP HANA
- 資料保護圖
- 持續資料防護

ADVANCED DISASTER RECOVERY 3月31日

- 生產和測試容錯移轉
- 僅雲端和站台對站台 VPN 連線
- 多個範本
- 網路保護的災難復原*
- Runbook

ADVANCED FILE SYNC AND SHARE Q2 2021

- 公證和電子簽章
- 文件範本*
- 內部部署內容存放庫 (NAS、SharePoint)*
- 同步和共用檔案備份*

變更遊戲規則的防護

Acronis Cyber Protect Cloud

安全性

- #CyberFit Score
- 弱點評估
- 主動防護
- 不具本機簽章型偵測的防毒和反惡意軟體保護
- 裝置控制

NOTARY (隨用隨付)

管理

- 工作負載的群組管理
- 集中式計畫管理
- 遠端桌面
- 遠端協助
- 硬體清查

備份 (隨用隨付)

- 檔案備份
- 映像備份
- 應用程式備份
- 網路共用備份
- 備份至雲端儲存
- 備份至本機儲存

災難復原

- 測試容錯移轉
- 僅雲端 VPN 連線

檔案同步和共用 (隨用隨付)

工作負載

* 即將上市

Acronis

Cyber Foundation

建造知識更為博學的未來

#CyberFit

與我們一起創造、
傳播保護知識！

www.acronis.org

建造學校 • 提供教育方案 • 出自書籍