DATA SHEET

Thunder SSLi

TLS/SSL 解密提供即時可視性，協助掌握加密流量

A10 Thunder® SSL Insight® (SSLi®) 是全方位的 TLS/SSL 解密解決方案，可橫跨所有連接埠解密流量，協助第三方安全裝置分析所有企業流量，無需犧牲效能。

消除盲點

Thunder SSLi 可消除 TLS/SSL 加密造成的盲點，將耗用大量 CPU 資源的解密及加密功能從第三方安全裝置卸載，同時確保遵循各種隱私標準。

雖然專屬安全裝置能夠深入檢測及分析網路流量，但並非設計用於高速解密及加密流量。許多安全產品其實完全沒有能力解密流量。因此 Thunder SSLi 可協助擴增現有安全裝置，保障您的安全基礎架構投資，同時進一步強化您的零信任策略。

Thunder SSLi 可大幅提升基礎架構效能，將流量解密並轉送至一個以上的第三方安全裝置，例如新一代防火牆、入侵防禦系統 (IPS)、進階威脅防護 (ATP) 或其他解決方案。Thunder SSLi 可重新加密流量，並將其轉送至預定目的地。回應流量也是以相同方式接受檢測。

A10 Control 能夠橫跨多個網站簡化 Thunder SSLi 的運作和管理工作。A10 Control 配備完整全面的儀表板，即時提供可採取行動的見解掌握網路流量特性，並依據服務、應用程式類型、URL 類別及各種項目進行豐富分析，實現擴增零信任策略所需的可視性及控制能力。

平台

實體設備

虛擬設備

管理

A10 Control
集中分析和管理

深入瞭解

A10Networks.com/ssli

©2025 A10 Networks, Inc. 保留所有權利。

優勢

一次解密

多次檢測

利用 A10 SSL Insight 技術解密 SSL 流量，並將其轉送至第三方安全裝置進行檢測。

利用整合式負載平衡達到最高的正常運作時間，提升安全基礎架構能力，並讓防火牆及其他安全裝置不必再負擔需要大量運算的 SSL 加密工作，專心從事偵測及阻止攻擊。

解密流量

適用於任何安全裝置

如欲真正確保企業網路安全，避免各種內部及外部威脅，組織需要藉助各式各樣的安全裝置。

Thunder SSLi 能夠與主要安全廠商搭配運作，以多種方式部署於「安全解密區域」，確保整個網路安全無虞，對抗各種加密威脅。Thunder SSLi 能與下列項目互相操作：

- 防火牆
- 安全網路閘道 (SWG)
- 入侵防禦系統 (IPS)
- 統一威脅管理 (UTM) 平台
- 資料遺失防護 (DLP) 產品
- 威脅防護平台
- 網路鑑識及網路監控工具

降低

營運成本

Thunder SSLi 以集中點解密企業流量，並將其轉送至許多內聯和非內聯安全裝置。這樣可以消除各個安全裝置的解密負擔、提升效能，同時維持適當的安全調查，此外也無須為了支援耗用大量資源的解密及加密功能，而購買更大型的安全裝置。

獲得完整可視性

掌握盲點狀況

Thunder SSLi 解密流量的範圍橫跨所有連接埠及多種通訊協定，可消除加密盲點，讓安全基礎架構能夠檢測之前不可見的流量、偵測隱藏威脅並加以防禦。

驗證

憑證狀態

攻擊者可利用無效憑證滲透網路。如果未能封鎖這類攻擊，使用者就有風險遭受多種攻擊。

Thunder SSLi 支援憑證撤銷清單 (CRL) 及線上憑證狀態通訊協定 (OCSP)，可協助系統確認由伺服器接收的憑證是否有效。這有助於驗證原始憑證是否有效。

確保

法規遵循及隱私

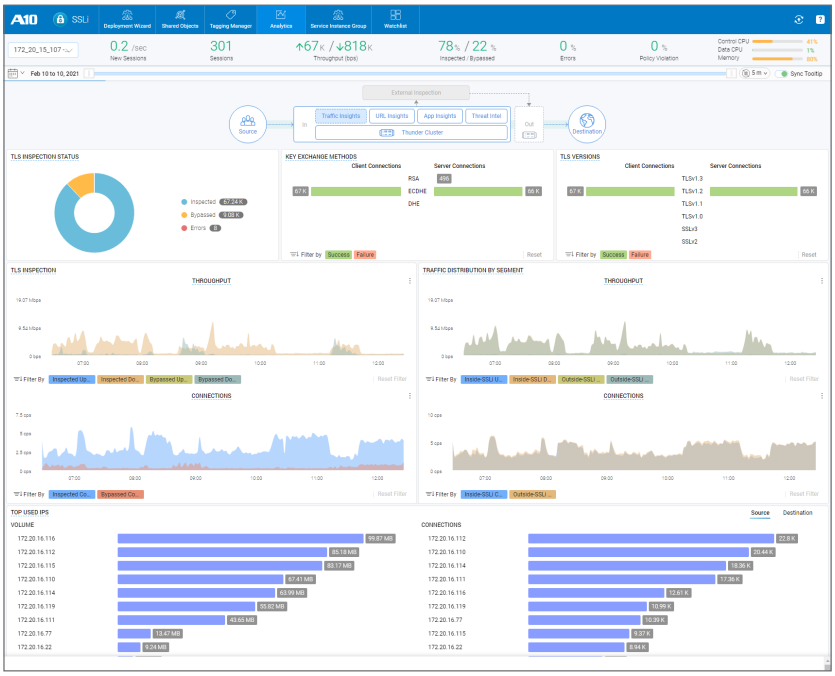
Thunder SSLi 可選擇性解密，確保組織符合產業、政府及其他法規遵循和隱私標準，例如，HIPAA 法規遵循可能禁止解密私人和敏感的醫療保健資訊。

©2025 A10 Networks, Inc. 保留所有權利。

集中

分析和管理

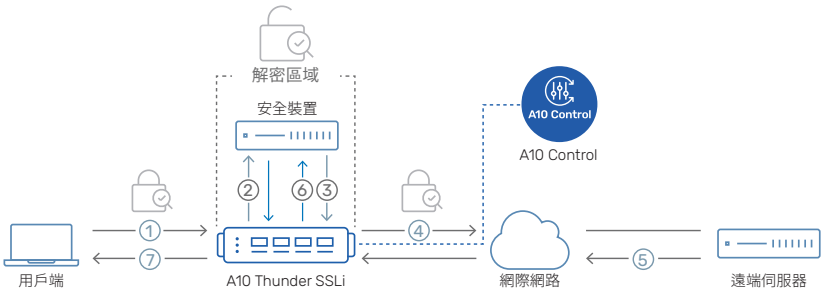
A10 Control 提供集中管理和豐富分析功能，可讓多個分公司的多個 Thunder 裝置結合成為一個集中及濃縮的控制台。分散式 Thunder 裝置可由中央位置透過 A10 Control 進行配置和管理。A10 Control 可顯示個別 Thunder 裝置統計資料，或彙總至直覺操作的儀表板之中，協助加速疑難排解並進行豐富分析。



A10 Control SSLi 應用程式提供全面完整的分析功能，協助以完整可視性掌握所有 SSLi 部署，並提供直覺操作的部署精靈，以及各種疑難排解工具。分析儀表板可個別填入用於各個 SSLi 執行個體，或以彙總方式提供全面檢視的流量模式。

©2025 A10 Networks, Inc. 保留所有權利。

參考架構



① 用戶端的加密流量由 Thunder SSLi 攔截並解密。

② Thunder SSLi 將解密流量傳送至安全裝置，以明文格式進行檢測。

③ 安全裝置完成檢測後，將流量送回 Thunder SSLi 以便攔截及重新加密流量。

④ Thunder SSLi 將重新加密的流量傳送至伺服器。

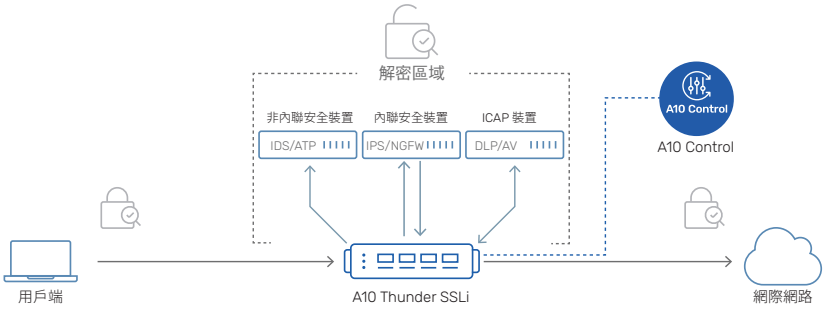
⑤ 伺服器處理要求，並將加密的回應傳送至 Thunder SSLi。

⑥ Thunder SSLi 解密回應流量，並將其轉送至相同的安全裝置進行檢測。

⑦ Thunder SSLi 接收安全裝置傳送的流量，重新加密後傳送至用戶端。

流量通過解密區域的流程

Thunder SSLi 透過邏輯解密區域提供可視性，第三方安全裝置會在解密區域內檢測流量是否具有威脅。Thunder SSLi 可部署為單或雙設備配置。



多種部署及解密選項

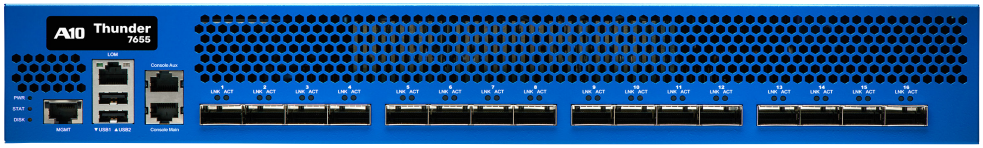
Thunder SSLi 可內聯部署於企業周邊，並可同時為多種安全產品解密流量，包括內聯、非內聯 (被動 / TAP) 及支援 ICAP 的裝置。

Thunder

7655S SSLi

重要數據

72 Gbps	145 Gbps	4M	100
SSLi 處理量	SSL 批量處理量	SSLi 同時連線	GbE 連接埠



RSA：100K
ECDHE：70K
SSLi CPS

©2025 A10 Networks, Inc. 保留所有權利。

適合任何安全裝置的解密流量解決方案

防火牆

- Cisco FirePOWER
- Palo Alto Networks 新一代防火牆
- Check Point 新一代防火牆

安全網路閘道

- Symantec Edge SWG
- Forcepoint Trusted Gateway System

進階威脅防護

- FireEye Network Security
- Fidelis Network

鑑識及安全系統

- RSA NetWitness
- IBM Security QRadar

入侵防禦系統

- Trellix IPS (McAfee NSP)
- Secureworks iSensor

其他

- OPSWAT MetaDefender
- Trend Micro Deep Security
- Vectra NDR
- Garland Technology NPB
- Niagara Networks NPB/Bypass Switch

特色

解密

橫跨多個連接埠及通訊協定

Thunder SSLi 使用動態連接埠檢測功能，可在任何 TCP 連接埠解密一般 TLS 流量。

此外也支援在其他安全服務通訊協定進行解密，例如 STARTTLS、XMPP、SMTP 及 POP3。然而解密功能並不是僅限於 SSL/TLS，也支援加密流量及解密 SSH 流量。

完整代理

架構

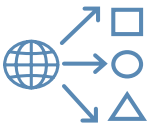
Thunder SSLi 以完整代理的方式運作，因此可調整用於加密的加密套件選項。Thunder SSLi 能夠重新協商至類似強度的不同加密套件，讓解決方案能夠符合未來需求，因應網路上未知的新型加密或 TLS 版本。Thunder SSLi 可確保流量以最安全的密碼進行加密，不會使用遭到破解的密碼。

©2025 A10 Networks, Inc. 保留所有權利。

多種密碼

提供 PFS 支援

Thunder SSLi 配備專屬 SSL 加速硬體，以 2048 位元及 4096 位元金鑰大小提供高效能，同時支援 DHE DHE、ECDHE、ECDSA 及 ChaCha-Poly 等各種進階加密套件，可支援完整轉寄密碼 (PFS)。



URL 分類

提供選擇性解密

Thunder SSLi URL 分類功能可將 10 億個以上網域的流量分門別類，選擇性略過流量解密以執行隱私原則，讓私人 / 敏感資料 (例如醫療或金融記錄) 不會遭到解密，並遵循 HIPAA 等法規遵循標準。

URL 篩選

提供存取控制

URL 篩選可協助員工達到最高生產力並降低風險，其中可封鎖存取惡意網站，包括惡意軟體、垃圾郵件及網路釣魚來源。

負載平衡

安全裝置

Thunder SSLi 支援負載平衡，可大幅提升防火牆及其他安全裝置的效能。可輕鬆新增安全能力，並延長現有安全裝置的使用壽命。可指派彈性的權重流量優先順序。

明確代理

部署支援

Thunder SSLi 除了標準的透明代理部署方式，也能以明確代理的方式部署，協助加強掌控流量管理。Thunder SSLi 可使用代理鏈連線至多個上游代理伺服器。

應用程式流量

辨識及控制

於應用程式層級識別及分類流量，以便更精細地控制及定義原則，並享有應用程式可視性和控制能力。此項功能搭配全方位的使用者及群組感知，可提供深入見解掌握應用程式流量，以便進行有效的安全規劃，並核准允許的業務應用程式。

ICAP

支援

資料遺失防護 (DLP) 系統一般會使用 ICAP 連線網路，協助預防未授權的資料外流。Thunder SSLi 除了支援 ICAP 連線能力，也同時支援其他解密模式。這樣網路現有的 DLP 系統就不必購買額外解決方案。

精細的

流量控制

使用 A10 aFleX® 指令碼檢驗、更新、修改或丟棄要求 DPI。完全掌控要攔截的流量，並轉送至第三方安全裝置，以及控制哪些流量需要先進行清理，然後再傳送至預定目的地。

©2025 A10 Networks, Inc. 保留所有權利。

智慧服務鏈

提供高效能安全性

依據應用程式類型以精細原則選擇性重新導向流量至不同服務鏈。Thunder SSLi 只要**解密一次**就能**檢測多次**，因此可以整併解密和加密工作，進而減少延遲及潛在瓶頸。

使用者驗證及使用者型原則

可為使用者建立安全原則，確保不允許任何未授權存取，並具備身分及存取管理功能。這也能讓您定義以使用者 ID 為基礎的流量及檢測原則，以維持精細控制。

威脅情報

IP 威脅情報源可協助識別及封鎖傳入和傳出已知不良 IP 位址的流量，甚至在進入解密流程之前就可進行。

Threat Investigator 可依據威脅信譽及信心分數以探索及確認網站的可信任度。此項功能可透過 A10 Control 存取使用。

集中分析和管理

A10 Control 提供裝置健全狀態、日誌及流量模式分析等功能，協助您監控效能並加速疑難排解。

企業可透過深入見解掌握異常狀況及威脅，以便透過行為分析設定自適應的控制和原則更新。

©2025 A10 Networks, Inc. 保留所有權利。

Thunder SSLi 實體設備規格

效能	Thunder 1060S-10G SSLi	Thunder 1060S SSLi	Thunder 3350S SSLi
SSLi 處理量	1 Gbps	2 Gbps	5.5 Gbps
SSLi CPS	RSA：2K ECDHE：1.2K	RSA：6K ECDHE：4K	RSA：20K ECDHE：10K
SSLi 同時連線	50K	100K	300K
SSL 批量傳輸量*5	10 Gbps	15 Gbps	30 Gbps
網路介面			
1 GE (BASE-T)	7	7	6
1 GE 光纖 (SFP)	0	0	2
10/1 GE 光纖 (SFP+/SFP)	4	4	8 + 4*4
25/10 GE 光纖 (SFP28/SFP+)	2	2	0
40 GE 光纖 (QSFP+)	0	0	0
100/40 GE 光纖 (QSFP28/QSFP+)	0	0	0
管理連接埠	乙太網路管理連接埠、RJ-45 主控台連接埠		
硬體規格			
處理器	Intel 通訊處理器 20 核心 [9 核心作用中]	Intel 通訊處理器 20 核心	Intel Xeon 14 核心
記憶體 (ECC RAM)	32 GB [24 GB 作用中]	32 GB	64 GB
儲存裝置	SSD		SSD
硬體加速	軟體		軟體
TLS/SSL 安全加速	硬體		硬體
尺寸 (吋)	1.75 (H) x 17.5 (W) x 17(D)		1.75 (H) x 17.5 (W) x 18(D)
機架單元 (可安裝)	1U		1U
單元重量	12 lbs		18 lbs
電源 (提供 DC 選項)	雙 300W RPS		雙 750W RPS
	80 Plus Platinum 效率，100 - 240 VAC，50 - 60 Hz		
耗電量 (典型/最大)*2	112W / 127W		175W / 222W
每小時熱量 (典型/最大) (單位：BTU)*2	383 / 434		598 / 758
冷卻風扇 (從前到後的氣流)	可拆式風扇		熱插拔智慧風扇
作業範圍	溫度 0° - 40° C	濕度 5% - 95%	
法規認證	FCC Class A, UL, ICES, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS		FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM | RoHS, FIPS 140-2*
標準保固	90 天硬體與軟體保固		

©2025 A10 Networks, Inc. 保留所有權利。

Thunder SSLi 實體設備規格 (續)

效能	Thunder 6655S SSLi	Thunder 7655S SSLi
SSLi 處理量	36 Gbps	72 Gbps
SSLi CPS	RSA：50K ECDHE：35K	RSA：100K ECDHE：70K
SSLi 同時連線	2 Million	4 Million
SSL 批量傳輸量*5	72.5 Gbps	145 Gbps
網路介面		
1 GE (BASE-T)	0	0
1 GE 光纖 (SFP)	0	0
10/1 GE 光纖 (SFP+/SFP)	0	0
25/10 GE 光纖 (SFP28/SFP+)	0	0
40 GE 光纖 (QSFP+)	0	0
100/40 GE 光纖 (QSFP28/QSFP+)	16	16
管理連接埠	乙太網路管理連接埠、RJ-45 主控台連接埠、無人值守管理	
硬體規格		
處理器	Intel Xeon 28 核心	2 個 Intel Xeon 28 核心
記憶體 (ECC RAM)	192 GB	384 GB
儲存裝置	SSD	SSD
硬體加速	FTA-5，SPE	2 個 FTA-5，SPE
TLS/SSL 安全加速	硬體	硬體
尺寸 (吋)	2.625 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
機架單元 (可安裝)	1.5U	1.5U
單元重量	39 lbs	44.2 lbs
電源 (提供 DC 選項)	雙 1500W RPS	
	80 Plus Platinum 效率，100 - 240 VAC，50 - 60 Hz	
耗電量 (典型/最大)*2	667W / 856W	1,121W / 1,300W
每小時熱量 (典型/最大) (單位：BTU)*2	2,276 /2,921	3,826 / 4,436
冷卻風扇 (從前到後的氣流)	熱插拔智慧風扇	
作業範圍	溫度 0° - 40° C	濕度 5% - 95%	
法規認證	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS, FIPS 140-2+	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS, FIPS 140-2+
標準保固	90 天硬體與軟體保固	

Thunder SSLi 已完全整併至 A10 Thunder CFW 產品系列。請參閱 Thunder CFW data sheet 瞭解更多 SSL Insight 解決方案產品。

硬體規格和效能數據如有變更，恕不另行通知，並且可能因配置和環境條件而異。對於網路介面，強烈建議使用 A10 Networks 的合格光學/收發器，以確保網路的可靠性和穩定性。

所有 SSLi 產品也可透過 CFW 授權提供。SWG 使用案例 (例如應用程式感知防火牆和 IP 威脅情報) 需要 CFW 產品系列。

*1 於單一設備 SSLi 部署搭配最大 SSL 選項的情況下測試。含 RSA 2K 密鑰的密碼「TLS_RSA_WITH_AES_128_CBC_SHA256」用於 RSA 案例，含 EC P-256 及 RSA 2K 密鑰的「TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256」用於 ECDHE 案例。
*2 基本型號。數量因 SSL 型號而異 | *3 提供可選的 RPS | *4 僅 10Gbps 速度 | *5 使用最大 SSL 選項的總 SSL (交易) | ^ 認證中 | + 必須購買 FIPS 型號

©2025 A10 Networks, Inc. 保留所有權利。

Thunder SSLi 虛擬設備規格

vThunder SSLi	
支援的 Hypervisor	VMware ESXi (VMXNET3、SR-IOV、PCI Passthrough)、KVM QEMU (SR-IOV、PCI Passthrough)
硬體要求	請參閱安裝指南
授權*	• BYOL 頻寬授權 • FlexPool 授權
標準保固	90 天軟體保固

* 頻寬授權需依據通過 SSLi 設備的總流量進行應用。例如單一設備 SSLi 部署會交易流量兩次 (用於解密及重新加密)，因此實際頻寬可能達到 SSLi 傳輸量的兩倍以上。在一次交易中進行兩次 (用於解密和之後的重新加密)。

©2025 A10 Networks, Inc. 保留所有權利。

詳細功能清單

功能可能因設備而異。

偵測/分析

- 高效能 SSL 解密及加密作為正向代理
- 完整代理架構
- 網際網路內容調適通訊協定 (ICAP) 支援搭配預先篩選用於資料遺失防護 (DLP) 及防毒解決方案
- 以動態連接埠解密偵測及攔截 SSL 或 TLS 流量，不受 TCP 連接埠編號影響
- 以雙向檢測保護對抗傳入 Web 威脅
- 以正向代理失效安全在交握失敗時略過流量
- 依據主機名稱略過解密；略過清單可擴充達到 1 Million 伺服器名稱指示 (SNI) 值
- 支援多個略過清單
- 廣泛的密碼及通訊協定支援
  - SSL 3.0、TLS 1.0/1.1/1.2/1.3*3
  - RSA/DHE/ECDHE/ECDSA/ChaCha-Poly 密碼搭配完整轉寄密碼 (PFS) 支援
  - SHA、SHA-2、MD5 訊息驗證碼 (MAC) 演算法
  - IPv4 及 IPv6
  - HTTP 1.1、HTTP/2
- 解密 HTTPS、STARTTLS、SMTP、XMPP、POP3、SSH、SCP、sFTP
- 用戶端憑證偵測及選用略過功能
- 非信任/過期憑證處理使用：
  - 線上憑證狀態通訊協定 (OCSP)
  - 憑證撤銷清單 (CRL)
- 詳細的使用者及連線記錄
- 使用者驗證及授權服務用於身分型存取控制
- SaaS 本地卸載和存取控制
- 下一個跳躍點負載分佈 (NHLD) 用於網際網路流量負載分佈及最佳化
- TLS 警示記錄用於記錄 SSLi 事件的流量資訊
- SSL 工作階段 ID 重複使用
- aFleX 指令碼提供可自訂的應用程式感知切換
- 高可用性：主動-主動、主動-待機配置
- 防火牆負載平衡 (FWLB)

URL 分類*2

- URL 略過提供以 Web 類別為基礎的選擇性解密
- URL 篩選用於封鎖已知惡意或不良網站

威脅情報*2

- IP 威脅情報服務*1 可依據可自訂的風險分數及容錯程度，預防惡意流量進入網路
- Threat Investigator 提供豐富的情境式分析，適用於 URL、IP 及應用程式等物件

應用程式感知防火牆*1| *2

- 可識別應用程式內部的服務類型，以辨識數以千計的通訊協定特徵
- 支援即時執行的自訂規則

部署

- 內聯透明代理或明確代理部署搭配非內聯第三方裝置
- 內聯透明代理或明確代理部署搭配內聯第三方裝置
- 內聯透明代理或明確代理部署搭配 ICAP 連線裝置
- 內聯透明代理或明確代理部署搭配使用代理鏈的第三方透明及明確代理裝置

虛擬化

- 適用於 VMware vSphere ESXi、Microsoft Hyper-V 及 KVM 的 vThunder 虛擬設備
- Dell Technologies OEM 解決方案套件上的 A10 Thunder

管理

- 專屬內建管理介面 (GUI、CLI、SSH、Telnet)
- SNMP、Syslog、電子郵件警示
- RESTful API (aXAPI)
- LDAP、TACACS+、RADIUS 支援
- 可配置的控制 CPU
- 可與 A10 Control 互相操作，以實現集中管理、配置和分析

透過 A10 Control 提供集中管理和分析

- 跨越多個網站的裝置及配置管理
- 提供引導式配置的部署精靈
- 集中安全原則管理及執行
- 豐富的 TLS/SSL 流量及解密分析，提供流量見解、應用程式見解、URL 見解、來源及目的地見解和其他資訊
- Threat Investigator 檢視
- 連線記錄檔深入分析
- 疑難排解工具

* 功能可能因設備而異。
*1 於 CFW 平台/授權提供。
*2 需要軟體及服務訂閱。
*3 於 Thunder 1060S、3350S、6655S 及 7655S 提供。

關於 A10

A10Networks.com

聯絡我們

apac@a10networks.com

©2025 A10 Networks, Inc. 保留所有權利。A10 Networks、A10 標誌、A10 Control、A10 Defend、A10 Harmony、Harmony、A10 Thunder、Thunder、ACOS、A10 SSL Insight、SSL Insight、SSLi、vThunder、ThreatX 和 ThreatX Protect 是 A10 Networks, Inc. 或其關係企業在美國和其他國家/地區的商標或註冊商標。所有其他商標均為其各自所有者的財產。A10 Networks 對本文件中的任何不精確處不承擔任何責任。A10 Networks 保留變更、修改、轉讓或以其他方式修訂本出版品的權利，恕不另行通知。有關商標的完整清單，請造訪：A10Networks.com/a10trademarks。

Part Number： A10-DS-15113-TW-30 November 2025

請按讚並追蹤 A10 facebook粉絲專頁