



Imperva Incapsula 雲端應用交付服務

安全是 Incapsula 的核心
安全是 Incapsula 的DNA，並融入一切產品服務中。Incapsula 在2009年由一群專注在網路應用程式安全的資深資安人員所成立；2014年正式被Imperva納入旗下，成為 Imperva 全資子公司。目前，全球數以萬計的企業都用 Imperva Incapsula 來保護、加速他們的網站和網路應用程式 - 無論是中小型企业、電子商務網站，或是大型、高度安全導向的SaaS供應商和金融機構。

無論您是進行小規模的電子商務或是大型企業的IT營運，Imperva Incapsula 都能增進您的網站安全與效能。透過雲端服務的方式，Incapsula 減少硬體與應用程式管理的負擔，並提供超越傳統內部解決方案的有力工具。

Imperva Incapsula 提供符合企業需求的網站安全選項和效能服務

無論你需要的是網路應用程式防火牆，或是 DDoS 防護、CDN 或負載平衡解決方案，Incapsula 都能提供。這種全方位的應用交付解決方案能讓企業將不同服務和設備整合到單一企業級的雲端服務中，以簡化IT營運流程並降低成本。Incapsula 是以雲端為基礎的應用交付服務，讓各種規模的線上業務都能享有企業級的網站安全、效能和可用性。Incapsula 提供最佳的網路應用程式防火牆、完整的 DDoS 防護、全球內容傳遞網路 CDN 和應用層負載平衡器，均可作為個別獨立服務或整合性解決方案。只需透過簡單的 DNS 變更即可啟用，不需安裝軟硬體、修改程式或其他複雜的整合。

Incapsula 雲端應用交付服務



DDoS
流量清洗



網站防護



CDN 與
最佳化器



負載平衡器

DDoS 防護

自動緩解最大量和最智慧化的DDoS攻擊

全面防禦所有型態的DDoS攻擊

Incapsula 以遍佈全球的高容量網絡，保護企業網站免於各種DDoS威脅，包括網路層攻擊（如SYN 或 UDP Flood）和企圖消耗伺服器資源的應用層攻擊（如GET Flood）。Incapsula 服務可以檢測、緩解利用應用程式、網路伺服器和DNS 伺服器漏洞所進行的進階攻擊和大型殭屍網路威脅。

透明緩解（Transparent Mitigation）

Incapsula 以低於0.01%的誤報率提供透明緩解服務，且不影響正常用戶使用，讓您享有真正的DDoS防護。即使遭遇長時間的攻擊，也不會造成業務中斷。

自動檢測、即時觸發與層級攻擊進階緩解

Incapsula 的來源識別技術（visitor identification technology）能區分網站正常來源（訪客、搜尋引擎等）和自動、惡意來源，並能區分人與Bot的流量、“好”與“壞”Bot的不同，辨別AJAX和API。

DNS 防禦功能

Incapsula 將網域內所有的DNS查詢重新導向 Incapsula 雲端，並進行檢查和過濾，以防禦針對DNS所發動的攻擊，因此只有“安全”的查詢會到達原本的DNS伺服器。此外，若有惡意連結測試，想將您的DNS伺服器作為攻擊其他伺服器的跳板，也會被此功能阻擋攔截。

BGP 路由基礎設施防護

為保護整個 IP subnet 裡的關鍵基礎架構（如Web、電子郵件、FTP伺服器），Incapsula 提供基於BGP路由的DDoS客製化防護。遭受攻擊時，流量將透過具有BGP公告訊息的 Incapsula 清洗中心重新傳輸，完成檢查後，正常的流量便會透過GRE通道安全地傳到企業網路。

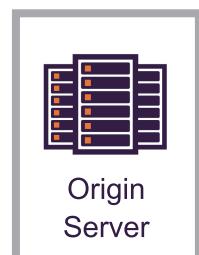
DDoS 和資安專家提供的全球支援

Incapsula 經驗豐富的網路維運中心（NOC）工程師團隊會持續進行監控和DDoS緩解。這項服務包含主動安全事件管理與回應、不間斷的實時監控、策略調整、攻擊報告摘要和24x7的技術支援。



可保護的伺服器類型

WEB
SSL, FTP, Telnet
SIP
SMTP
UDP, TCP
DNS



Origin
Server

網站安全

來自雲端的企業級防護

Incapsula 透過先進的分析功能提供強大的網路應用程式安全體驗，為全球所有注重資安的企業提供最佳的安全防護。Incapsula 的網站防護解決方案重新定義並擴展超越傳統概念的WAF，其進階來源分類引擎會分析所有傳入企業網站的流量，防止惡意和不必要的存取。

What You Get

- 最高等級、PCI 認證的網路應用程式防火牆
- 可依企業安全政策及使用環境進行客製化設定
- 提供網路存取雙因素驗證
- 可分析所有進入流量的客戶分類引擎
- 易於和後端系統整合的API



企業級網路應用程式防火牆 (WAF)

Incapsula 企業級、PCI 認證的 WAF 能保護您的網站或應用程式免於應用層的入侵攻擊。結合 Imperva 領先業界的 WAF 技術與經驗，Incapsula 以雲端為基礎的 WAF 能抵禦包含OWASP 十大威脅等各種網路攻擊及弱點，同時並能依企業組織的安全政策在 WAF 中設定客製化的安全規則。

進階 Bot 流量緩解

透過來源分類技術、群眾外包 (crowdsourcing) 及信譽評等技術 (reputation-based technique)，Incapsula 能辨別“好”與“壞”的 Bot 流量，讓您可以阻擋讓伺服器超載並竊取資料的駭客與垃圾訊息發送者，同時讓搜索引擎和其他服務能正常存取網站。

雙因素驗證

不須系統整合、調整程式或軟體，即可滿足網站或應用程式所需的雙因素驗證。只要一鍵啟用，就能保護管理者存取、公司網路應用程式遠端存取並限制特定網頁存取，同時可集中管理跨網站的多重登錄。

網站存取管控

能充分管控存取網站的人或應用程式。透過細項篩選及管控過濾掉不必要的來源（如國家/地區、特定Bot、URL、IP等），並維持正常來源的存取（如客戶、主要搜索引擎等）。IP位址屏蔽則能隱藏您的網路伺服器IP位址。

Incapsula 企業計畫

Incapsula 專家了解企業網路應用程式的運作方式，並和企業IT團隊密切合作，以滿足不同的整合與客製化要求。在企業級 uptime SLA 和完整支援下，Incapsula 點到點應用交付服務可以最大化網站和網路應用程式的安全性及效能，而整合多種設備和服務的單一解決方案也能讓企業簡化IT運作流程並降低成本。

Incapsula 主要企業服務項目包括：

- **企業級SLA**

Incapsula 了解服務是沒有妥協空間的，在 99.999% uptime 及 SLA 的基礎下，Incapsula 優異的企業級網站安全及效能服務廣被全球領先的電子商務選用。

- **24x7 全天候支援**

Incapsula 的技術工程師及資安專家全天候隨時提供企業所需的支援。

- **企業級防護**

藉由 PCI 認證的 WAF 和完整的 DDoS 攻擊防護，Incapsula 能保護企業網站免於外部攻擊，最大化 uptime 並維持業務連續性。

- **專為佈建、管理和安全事件所設計的 API**

Incapsula API 能輕易整合並簡化客戶佈建流程和帳戶管理，並能將安全事件匯出到 log 管理和SIEM系統，為企業目標受眾建立客製化的報告內容。

- **客製化設定與頁面設計**

Incapsula 的客製化選項能讓企業配合網站的品牌形象，輕鬆設定、設計面對末端客戶的頁面（如安全訊息、錯誤頁面等）。

- **專用帳戶管理**

Incapsula 資安專家將協助您完成複雜的設定，並依需求提供量身訂製的產品服務，滿足您在營運及資安上的目標。

Incapsula客戶群包括

- SaaS 供應商
- 電子商務網站
- 貿易平台
- 遊戲平台
- 銀行
- 政府相關單位

基本選購方案	Cloud WAF	DDoS 防禦	Site Domain
Enterprise 20	20 M	選購	1 site
Enterprise 50	50 M	選購	1 site
Enterprise 100	100 M	選購	1 site