# SME Cloud Security

## 中小企雲端服務信息安全

# 中小企使用雲端服務實用保安指南

『中小企業發展支援基金』撥款資助
Funded by SME Development Fund

工業貿易署
Trade and Industry Department

主辦機構
香港中小型企業總商會
The Hong Kong General Chamber of Small and Medium Business

協辦機構
Hong Kong Software Industry Association
香港軟件行業協會

執行機構
PEAK
Member of VTC Group
VTC 機構成員

香港中小型企業總商會

香港中小型企業總商會
The Hong Kong General Chamber of Small and Medium Business

香港中小型企業總商會於1995年由職業訓練局轄下之香港中小型企業經營管理協會幹事所建立，是一個非牟利的工商社團民間組織。商會成員包括各行各業之中小型企業東主、專業人士及從事中小型企業研究的學者等。而其他對中小型企業有興趣之人士，亦可申請加入成為附屬會員。中小型企業之定義，是以僱員人數來劃分，聘用少於100 名員工的製造業公司和聘用少於50 名員工的非製造業公司，便屬於中小型企業。

本會旨在團結香港中小企業界，維護他們的權益，為他們爭取更佳的經營環境，提升香港中小企業的形象。同時，我們更為會員拓展業務網絡，製造商機、及致力提高企業管理質素及生產力，以增強自身競爭力。

# 目錄

關於計劃

編者語 頁

第1章 什麼是雲端服務 ..... 8

第2章 雲端保安(網絡篇)

2.1 內聯網、互聯網 WiFi 網絡設備 ..... 11
2.2 公眾網絡的使用 ..... 14
2.3 公司域名使用 ..... 16

第3章 雲端保安(用户端設備篇)

3.1 賬户登入管理 ..... 20
3.2 備份管理 ..... 21
3.3 防毒、補丁管理 ..... 23
3.4 設備管理 ..... 24

第4章 雲端保安(應用服務篇)

4.1 雲端硬盤 ..... 26
4.2 使用移動設備 apps 的保安事項 ..... 27
4.3 電郵 ..... 27
4.4 app stores ..... 28
4.5 網絡交易要注意的事項 ..... 29
4.6 瀏覽器保安事項 ..... 29

第5章 雲端保安(管理篇) ..... 30

第6章 用家分享

中小企電子商貿信息安全技術與實踐 — Alibaba.com 案例 ..... 32

第7章 雲端保安服務例子 ..... 35

聯絡

# 關於計劃

雲端服務、各種網上或電子商貿服務不僅可以加強業務運作效率，更幫助企業家探索和發掘新商機、新市場和新客戶，以及促進與客戶的溝通，維持和實現許多策略性業務目標，包括節約成本。

大部份中小企業明白雲端服務、網絡和電子商貿這些新科技帶來的好處，卻因為訊息和數據安全問題、沒有足夠的資源來評估、研究和學習必要的技能和知識，而猶豫不敢使用這些技術。

「提升香港中小企在資訊科技及雲端商用上的安全策略」培訓及諮詢項目計劃讓香港中小企業能掌握雲計算應用及服務的安全使用方法，在本地和全球化的商業環境中競爭。項目透過研討會、培訓、項目網站、簡單易明的手冊，及行業專家和從業者的經驗分享，讓中小企業能更安全和有效地使用可靠的雲端運算和電子商貿服務。

「中小企使用雲端服務實用保安指南」為本地中小企而設，列舉有關安全使用雲端服務和互聯網應用的資訊。

『中小企業發展支援基金』撥款資助
Funded by SME Development Fund

主辦機構

工業貿易署
Trade and Industry Department

香港中小型企業總商會
The Hong Kong General Chamber of Small and Medium Business

協辦機構

Hong Kong Software Industry Association

執行機構

PEAK
Member of VTC Group

合作/支持機構：(排名不分先後)

在此刊物上/活動內（或項目小組成員）表達的任何意見、研究成果、結論或建議，並不代表香港特別行政區政府、工業貿易署或中小企業發展支援基金及發展品牌、升級轉型及拓展內銷市場的專項基金（撥備支援計劃）評審委員會的觀點。

本計劃由香港特別行政區政府工業貿易署『中小企業發支援基金』撥款資助，香港中小型企業總商會(HKGCSMB)主辦，職業訓練局高峰進修學院(PEAK)執行。在此刊物上/活動內(或項目小組成員)表達的任何意見、研究成果、結論或建議，並不代表香港特別行政區政府、工業貿易署或中小企業發展支援基金及發展品牌、升級轉型及拓展內銷市場的專基金(機構支援計劃)評審委員會的觀點。

# 編者語

首先，筆者十分感謝香港中小型企業總商會及職業訓練局高峰進修學院給予機會參與「提升香港中小企在資訊科技及雲端商用上的安全策略」培訓及諮詢項目計劃，並策劃及執行一系列讓中小企業參予的雲端保安課程及活動; 在此特別感謝中信國際電訊安排我們的學員參觀雲端應用服務的主幹 — 數據中心，讓學員走出課室，了解數據中心如何為雲端數據提供物理保護(physical security)。

筆者自 90 年代初香港中文大學訊息工程系畢業以來，生活、工作跟互聯網絡可以說是共同成長及發展。網絡服務從本地網絡(local area network)到今天移動互聯網(mobile internet)及雲端網絡(cloud)，應用技術推陳出新; 不過，網絡保安漏洞、軟件病毒、黑客入侵等等亦從來沒有休止。筆者在 2000 年起已開始為商業機構及職業訓練局提供資訊科技保安的顧問及培訓服務，那些年大家比較着重管理公司內部網絡、伺服器的保安技術。今天，雲端服務漸漸普及，保安的重點轉移至應用軟件、計算機設備(包括手機 、平板電腦、智能電視等)及雲端應用服務。

筆者於 2009 年至 2011 年在阿里巴巴擔任 B2B 商業服務主管期間，在接觸本港中小企廠家及出口貿易商，經常提醒各中小企老闆在使用網站服務時，除了關注網上生意的營運，亦要特別留意網站賬號的管理。試想，即使你利用網絡找尋了許多做生意的好機會、數據、資訊，你不好好保護賬戶登入權限，你的員工、競爭對手或許十分容易取得商業機密。

筆者公司作為電郵服務供應商，曾經收到聲稱是一位客戶的管理層人員來電，他說因忘記密碼，要求更改電郵郵箱密碼; 幸好公司已訂立一套完善的保安守則，服務人員嚴格執行，只為客戶指定及已登記的聯絡人處理敏感資料，拒絕了該來電者要求; 事後我們知道該來電者是該公司剛離職的同事。

筆者相信，對中小企業來說，處理各雲端保安漸漸成為日常商業營運的必要事項。這本小冊子提供了一些簡單實用的雲端保安手段，希望能幫助各行業的中小企解決相關的問題。

本計劃得到一眾雲端服務的業界嘉賓提供的專業知識及資料，順利完成 10 課堂課程。如果你錯過了課堂，請到本計劃網站 http://cloud4smb.hk 瀏覽各課程內容的簡要及重點節錄。

李松英 雲端服務經理
2015 年 12 月
聯絡: cy.laps@yahoo.com.hk

本小册子得以完成，我們藉此機會感謝以下公司協助：
(按英文字母順序排列)

Ahsay Systems
Cisco Systems (HK) Ltd.
CITIC Telecom International
eBay International Hong Kong
F-Secure
HP
IBM China/Hong Kong
Intuit Quickbook
JSNA Asia Enterprises
Laps Solutions
Linking Business Network
PayPal Hong Kong
Readyspace
Towngas Telecom
Tredmicro

# 第1章 什麼是雲端服務?

雲端服務是建基於互聯網網絡及設備的服務。一般來說，互聯網是由網絡設備、電算機、儲存硬件及各式各樣的軟件構成。其實雲端不過是一個近年比較人氣的互聯網替代詞，事實上有互聯網服務的第一天開始，電子郵件應用、網頁應用已經可算是第一代的雲端服務。

近年流動網絡及設備長促發展對雲端服務的興起起了關鍵作用。互聯網及流動網絡技術的發展，令互聯網從家居、商業環境下的在線服務走進流動電話網絡世界; 3G、4G 數據的傳輸速度近年大躍進，數據月費達到一般市民大眾可接受的價格水平; 另外，自蘋果 2007 年發佈 iPhone 以後，流動設備數量急促增長，在各領域互動發展下，互聯網服務或雲端服務持續發展。今天，平板電腦、智能手機的數量及增長速度已超越桌面電腦，個人或商業使用流動設備的時間相信大大超越昔日時候，各式其式的軟件將百花齊放，為龐大市場服務。對中小企業而言，企業營運、產品及市場開發，以至利潤都離不開如何善用雲端應用服務。

雲端服務並不是為跨國式、大企業而設。相反，過往許多企業級別的資訊科技應用成本高昂，入場門檻高，對中小企而言實在高不可攀，而大企業亦以此技術優勢佔據大份額市場。但是，雲端應用服務的特質是功能模塊化(modular)並提供針對性(targeting)的服務; 同時，雲端應用服務基建及開發成本可於全球市場攤分，對用户而言只須繳付服務年費或月費，即可享用企業級的資訊科技服務; 雲端應用服務令中小企業的競爭能力大大提昇。

雲端服務大致可分三類: 公有雲、私有雲及混合雲(public cloud, private cloud & hybrid cloud)。中小企業使用公有雲比較合適，其營運成本較低，技術要求對中小企而言相對簡單，適合一般缺乏資訊科技人力資源的企業。在私有雲或混合雲架構下，大企業則會自設網絡、伺服器或儲存設備、以至自己開發應用軟件，連接雲端服務供應商的網路或系統。

許多在互聯網線上服務多年的應用平台可說是公有雲服務的一種狀態。例如常用的免費郵箱 Google Gmail、Yahoo Mail 等服務，服務供應商於世界各

地設置了網絡設備、伺服器及儲存硬件，加上自家開發的軟件系統，為世界各地在線用户提供電郵服務。又如阿里巴巴的 Alibaba.com 網站服務，讓全世界買家、賣家增加搜尋對方、促成採購的機會。

從技術層面看雲端服務亦可分三類: 基建即服務(IaaS)、平台即服務(PaaS)及軟件即服務(SaaS)。基建即服務(IaaS, Infrastructure as a Service)指雲端服務供應商提供網絡連接、設備、伺服器及儲存設備租用; 平台即服務(PaaS, Platform as a Service)指除基建服務租用，用户可租用常用的作業系統(operating system)軟件如微軟視窗或 Linux，但是需要自行設置及管理應用軟件。

中小企業應大多會接觸及使用軟件即服務(SaaS, Software as a Service)，即用户按時或按量繳付服務費用，便可使用應用軟件服務。

軟件即服務也不是新事物。在雲端服務還沒有時興的時候，防毒軟件服務公司已經以年費的形式，向在線用户收取軟件更新服務費用; 用户繳納了費用，即可從互聯網下載最新的防毒軟件檔案。

## 雲端保安

前面提及公有雲及私有雲，許多人以為私有雲因硬件及作業系統軟件(如視窗系統)是私人配置，不跟他人分享資源，穩定性及安全性較公有雲佳; 其實這個說法較片面。事實上，許多資訊保安、黑客事故，從技術層面來看，多與軟件編程碼(programming codes)有缺陷(bugs)和漏洞(vulnerabilities)及欠缺軟件更新有關; 在操作層面上則與人為錯誤、疏忽有莫大關連，跟是否使用公有雲或私有雲算不上有直接連繫。


對中小企而言，由於在資訊科技的資源投入有限，認識不足，建立及管理私有雲算不上比使用公有雲好。相反，公有雲的雲服務供應商因商業市場因素令其不得不更專注、更有效能執行資訊保安手段，相對而言亦願意投入更多資源於資訊保安管理，中小企使用公有雲雲端服務比起自己建立、設置、維護 IT 設備絕對化算。

資訊保安可以說是資訊科技一個永恆的題目。由個人電腦從 70 年代盛行開始，軟件及電腦病毒是雙生兒。為什麼? 軟件創造者是編程人員，人並不完美，少不免會犯錯，很難想像會有一個滴水不漏、沒有缺陷和漏洞的軟件程式; 在互聯網及雲端時代，網絡的入侵或病毒的攻擊確實不能避免。對任何用户而言，資訊保安的管理就是一種風險管理，除非你跟互聯網世界脫離連繫，否則，你不能絕對免除受黑客侵襲的機會。

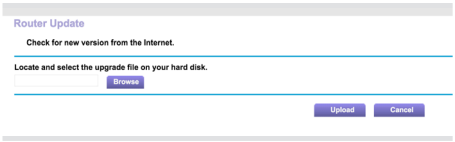
另一方面，你投入多少資源管理以減低這類風險及影響(risk & impact)，跟你從應用資訊科技所獲得的好處是一種平衡管理。資訊保安管理的特別之處是一個軟件系統保安手段的嚴緊度跟用户是否易於使用是一種矛盾: 一般情況下，方便了用户，資訊保安水平便下降; 嚴厲的保安手段往往嚇怕用家。這種現實是各類型用户包括中小企業要牢牢記着的原則，亦必須接受。

# 第2章 雲端保安(網絡篇)

中小企業要使用雲端服務，基建及硬件可能有以下的網絡配置:

- 內聯網 WiFi 網絡設備
- 互聯網連接
- 公眾網絡的使用(包括 WiFi 及流動數據網)
- 公司域名(Domain Name)使用

## 內聯網 WiFi 網絡設備




中小企業內聯網的保安手段離不開路由器(router)及防火牆(firewall)的使用。現在一般中小企業使用的路由器大部份都是多功能、可配置防火牆或其他網絡功能如 IPS (Intrusion Prevention Service)，以避免網絡襲擊。中小企業必須確定這些功能設置開啟，系統自動韌體更新(firmware update)亦須啟動。中小企業人手資源比較緊張，自動更新比手動更新較適合。

### WiFi 路由器

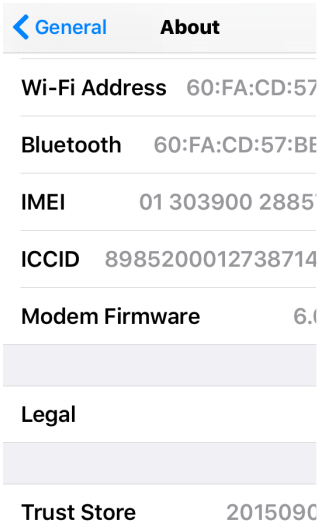
今天 WiFi 路由器(或稱為寬頻路由器, broadband router)是集互聯網連接、保安及 WiFi 網絡功能於一身。WiFi 網絡是一非實體連接(no physical connection)的網絡，對其保安手段的設置必須非常重視，無論是一般辦公室、工廈、家居的 WiFi 路由器，其保安設置應以最高等級的配置為目標; 以下列舉必要的保安措施:

1. 啟動系統自動更新
   跟使用路由器、防火牆硬件一樣，其原廠保安密碼必須更改，系統自動更新應該啟動。

2. SSID 的配置
WiFi 用户端為了搜尋正確的網絡使用，是以 SSID 識認; 比較保護私隱的做法是使用不容易顯示身份的 SSID 名字，例如避免使用公司名字。如果可以控制用户端 WiFi 設定的話，應預先鍵入 SSID，並隱藏 SSID 碼就更好。

3. 必須使用自己配置的 WiFi 加密系統
現時較常用、安全、中小企業易於執行的標準為 WPA2。WPA2 密碼會在用户端按入，請仔細考慮誰人可知其內容，將密碼備份並置於安全的地方，密碼亦應該定期更新。

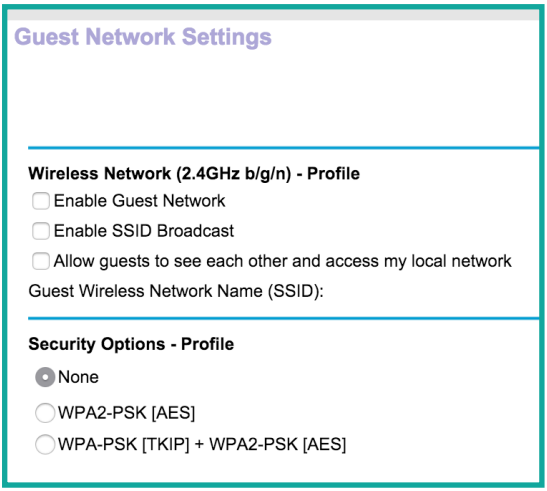
4. 用户端使用權限(access rights)
所有網絡設備(如桌面電腦、平板電腦、智能手機)必備有以太地址(Ethernet MAC Address)。中小企業可記錄各用户端設備的以太地址，集成一清單，並將按入路由器權限的設置上，強制路由器只可連接清單上的設備。




iOS 設備內，按：
> [設定]
> [一般]
> [關於手機]
可找 WiFi MAC address

5. 應該從內聯網利用瀏覽器設置路由器的配置。

6. 考慮到商業上訪客會使用公司的 WiFi 網絡，應選擇使用設有獨立訪客配置(Guest WiFi)的路由器，並設置 Guest WiFi 密碼，有訪客到來方告知其密碼，並定期更改。Guest WiFi 能獨立於公司 WiFi 內聯網，技術上令整個網絡系統私隱度較高。




即使是 Guest WiFi，緊記設置 WPA2 密碼。

## 互聯網連接

中小企業辦公室要通往雲端，租用電訊公司的寬頻上網必不可少。電訊公司會提供上網賬户名稱及初始密碼，一般情況下，你可利用寬頻網絡商提供的網頁設定版面更改賬户密碼; 如果其服務還提供互聯網保安的增值服務(如防火牆)，亦可於設定版面開啟使用。

另外，有些寬頻路由器提供虛擬網絡功能(VPN，virtual private network)，提供一個接口方便用户透過公眾網絡，接駁公司內聯網的伺服器或其他網絡設備(如遠端儲存設備 NAS，network access storage)。雲端服務尚未普及的時期，VPN 不失為遠端獲取公司數據、檔案及軟件應用服務的方案。但是從保安角度考慮，相關設備、系統繁復，較多的手動配置只會有更多機會

暴露保安弱點。所以對中小企而言，減少使用或避免自設的 VPN，並利用雲端服務實為最佳策略; 同時更應該把公司本地網絡(local area network)、內聯網(intranet)設備的遠端接口(remote access)完全關閉。

## 公眾網絡的使用(包括 WiFi 及流動數據網)

在流動辦公室年代，使用 WiFi 或流動數據上網必不可少。流動設備如智能電話、平板或手提電腦直接使用流動數據上網私隱性較高，原因是流動數據或電話的 SIM 咭，跟流動數據網絡商之間有較嚴格的用户認証及加密機制的傳訊通道。若不需考慮網絡費用及速度的限制，使用流動數據直接上網在安全角度較可取。同樣道理，其它流動設備使用流動咭配置 WiFi 熱點(hotspot)上網較佳。當然，WiFi hotspot 的安全設置即如設置你的辦公室 WiFi 一樣，小心處理配置 SSID 及 WiFi 密碼鑰(encryption key)也是必須的。

最近香港有一主題公園被人發現有許多 WiFi 熱點陷阱，黑客散播了若干免費上網的 WiFi 熱點吸引用家使用，相信黑客從無線網絡上搜集對其有價值的數據。若不是主題公園主動澄清尚未提供該服務，不知有多少用家的私隱信息會被盜竊。

如果有必要使用公眾 WiFi 網絡，請留意:

### 確認及核實正當的 WiFi 網絡(SSID) 名稱

首先要選擇及決定是否使用某一特定的 WiFi 網絡，譬如在一商場內，商場應透過線下渠道，列明 SSID 名稱，方便使用者查閱。當然在設備上看到的 SSID 也有可能是假冒的服務網絡。提供 WiFi 服務供應者絕對有責任及能力查核、監察是否有假冒的 WiFi SSID。在一般情況下，你唯有選擇相信服務者的管理能力。

因為是公眾 WiFi，服務商或服務提供者如商場管理公司，並不能為使用者預設 WiFi 密碼，所以你的設備與公眾 WiFi 網絡的渠道普遍是以非加密的數據傳輸，即是說你的設備傳送的數據絕對有可能暴露於 WiFi 服務範圍當中。

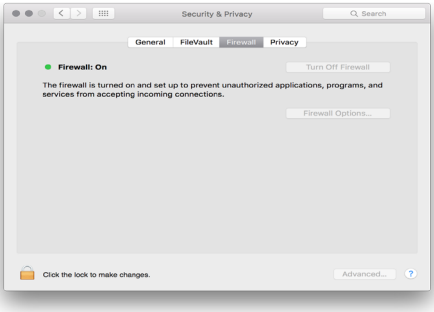
## WiFi 啟動密碼

有些公眾 WiFi 服務亦會分發使用 WiFi 啟動密碼，例如部分咖啡店會在銷售單據上列印了 SSID 及啟動密碼。但是，它有可能只用來管理及核實使用網絡的用戶，亦有機會不同用户使用同一條密碼鑰。無論如何，當你連接上一個公眾 WiFi 網絡，不論是或你的數據都是有機會暴露於 WiFi 網絡上。我們唯有依靠一些更高層次的數據加密機制如瀏覽器上的 https、SSL 等。


咖啡店會在銷售單據列印了 SSID 及啟動密碼

## 個人流動設備暴露於公眾網絡使用的保安要點

當你的設備暴露於公眾網絡、或一個不明的網絡上(例如你在別人公司網絡上使用自己的設備並獲取網絡服務)，你的資訊保安意識必要提高，下列是一般你應留意的事項及可執行的手段:




1. 使用或接上網絡前必須啟動個人設備的防火牆。手提電腦無論是視窗 Windows 或蘋果 Mac OS 各版本，都備有基本的防火牆設置，務必是長期啟動。
2. 沒有需要使用 WiFi 的話，請關閉流動設備無線網絡設置。你一旦選擇了使用某一個流動 WiFi，應避免剔選自動上網功能，以防止你在不知情況下流動裝置自動再次連接公眾網絡，減低被網絡侵襲的機會。
3. 當有必要進行互聯網數據傳輸之前，請儉查應用軟件程式是否使用加密渠道接駁雲端伺服器。最常用的方式是利用瀏覽器把訊息及資訊打包加密，加密機制以瀏覽器是否鎖上 (連結 https:// )為標示。

4. 使用公眾及户外網絡時應該避免進行處理跟私隱或敏感的資料及數據。
5. 在可信的網絡內，利用瀏覽器記憶功能(remember password)，先輸入各種應用服務為默認密碼。為什麼這樣做? 這可避免在公眾地方鍵入的重要登入信息及密碼，有機會被人窺視甚至攝錄。
6. 為了減低在公眾及不明網絡上受黑客入侵或網絡襲擊的風險，可選擇使用獨立於流動設備的第三方防毒軟件及 VPN 虛擬網絡服務。今天第三方的防毒軟件配置功能較完善的防火牆、IPS 及防網絡入侵的保安功能; VPN 服務可直接把用户端設備的數據加密，傳到可信賴的網絡服務器解密後跟互聯網連繫，無論從數據保密、保障私隱的角度看，保安程度大大提昇; 這種第三方提供的 VPN 虛擬網絡服務(例如芬蘭 F-Secure 的 Freedome)今天也是一類雲端服務。

## 公司域名使用 — 中小企業網絡身份的保護

網絡保安最重視之一是身份的認証，互聯網上中小企業的身份就是域名名字(domain name)。要擁有一個 .com、.hk 的域名年費低，申請手續簡便，但是中小企業往往忽略域名的管理，譬如因忘記繳納域名續期年費而導致電郵及網站失效，令公司營運停頓。另外，管理着域名伺服器服務的賬户可能只授權予唯一的員工或 IT 外判商，一旦員工離職或外判商不再服務，賬户的登入名稱、密碼、域名伺服器服務設定資料就完全遺失，更有可能被外界盜用，對業務造成極大不穩的風險。

公司的網域管理涉及電郵傳送及電郵伺服器正確位置的設定。假若網域及電郵設置落入黑客手上，任何以電郵地址作登入賬號所用的密碼有機會在用户未察覺情況下被更改，賬户即被黑客入侵。

域名管理有以下要注意的事項:

- 登記及申請 domain name 不應假手於人; 域名登記會記錄 3 方聯絡人: Registrant 、Technical、Administrative。企業擁有者必須至少登記為 Registrant; 另外兩個應為公司聯絡人，即使需要外判服務商協助，亦不可登記多個公司外的聯絡人。
- 管理 domain name 的賬户登入名稱及密碼一定要備份，即使是手寫下來也好，只要把線下的文件及數據安全地保存就可以了。

說起賬户登入名稱及密碼的管理，即使是中小企業大多數依賴外判服務公司或少數(甚至是唯一一位)內部 IT 員工，中小企老闆或管理層亦應該備份各服務登入名稱及密碼，例如網絡路由器的系統管理員、郵箱系統行政管理員、網頁管理員等等。 一旦有任何事故影響 IT 運作，需要委托第三方協助解決問題亦較易做到。

總之，原則是分權(separation of duties)，不可以把擁有權、管理服務、系統的行政權限只放在同一人或外判公司身上。

# 第3章 雲端保安(用户端設備篇)

使用雲端應用服務，尤其是中小企業多應用公有雲服務，除了網絡保安外，另外重點便放在用户端設備(End User Devices)上。

今天企業在辦公室上有座枱型電腦，流動工作有筆記型電腦、平板電腦及智能手機，各種用户端設備的保安手段亦有差異，我們先來了解一些共同的手段:

1. 作業系統(operating system)軟件應保持更新，無論是 Windows、Mac OS、iOS 或 Android 的設備，都應該開啟更新提示，時時留意。
2. 啟動個人防火牆及其他防毒軟件服務。
3. 啟用設備使用密碼，如果有如指紋辨識的生物特徵開機功能，應盡量使用。蘋果 iPhone 可設置 10 次輸入密碼嘗試，一旦輸入失敗，手機資料即自動銷毀，不能夠恢復使用。
4. 使用流動設備可開啟的硬碟加密功能(如視窗的 BitLocker、Mac OS 的 File Vault); 一旦硬體遺失，沒有密碼情況下盜竊者亦不能讀取設備硬碟中的數據及資料。

5. 安裝第三方防毒軟件。今天的防毒軟件功能多方面，更可同時提供防火牆、入侵防禦偵測、防毒掃描、郵件安全、網頁內容過濾等安全機制；同時應啟動軟件自動更新功能。

6. 使用廠家提供的雲端賬户(視窗、谷哥賬户、蘋果的 iCloud)，方便統一管理多部硬體；同時可啟用追蹤設備、遠端重設或刪除硬體數據(remote wipe)，對保障私隱有極大幫助。

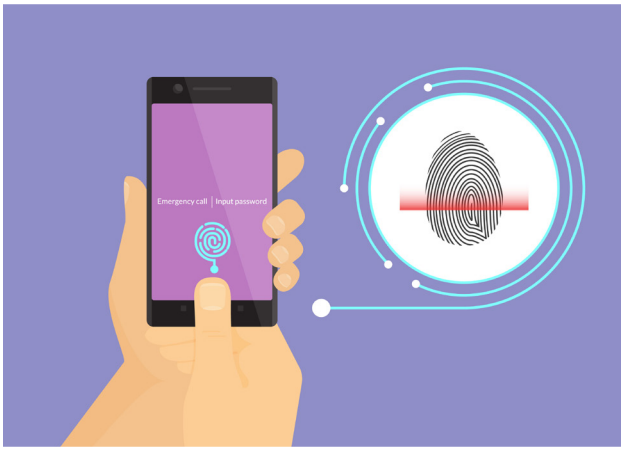
7. 今天在用户端使用瀏覽器獲取雲端服務必不可少，瀏覽器亦應啟動自動更新。另外，瀏覽器雖然可支援安裝許多外掛程式(plugin & extension)，應避免安裝。

8. 應盡量避免在瀏覽器使用默認密碼功能，尤其是用户端設備是與別人分享使用，以減少別人盜用你身份的機會。

9. 日常使用設備中，不可使用設備最高權限的賬户，以避免系統被入侵；不使用已越獄(jailbreak)的 iOS、已 root 的 Android 智能工具；另外，應該使用官網下載的應用軟件 apps(如 Apple Store 及 Google Play)，並按提示保持更新。

10. 用户端設備會安裝了無線連接功能如：藍芽 Bluetooth、近場識別通訊 NFC、Apple Airdrop、WiFi，在不使用情況下應把這些功能關閉，以減少保安漏洞。


11. 新近購買回來的桌面或筆記型電腦，尤其是從零售渠道購買的，有機會已安裝了大量原廠供應商提供的免費軟件；有先例指出這些軟件曾會窺探及洩露設備的數據予第三方，保安業界稱這些為臃腫軟件(bloatware/crapware/shovelware)。要減少使用設備的風險，可先卸下(uninstall)隨機附送而不必要的軟件，或者在採購時向供應商要求商用版硬體或微軟的 Signature PC。




使用指紋開關設備比使用記憶密碼作登入賬號更可取，除了是生物特徵難被冒認外，你亦不容易被人窺視按鍵而洩露密碼信息。但是，考慮是否洩露個人生物特徵數據又是另一層顧慮。現在指紋辨識大多數由流動設備生產商直接提供，選擇一件可信的硬件工具是關鍵。在不知名的硬體上啟動指紋辨識、讓工具套取你的重要私隱數據(例如手指模)，絕對是高危舉動。

另外，用户端保安手段亦可從以下管理方面考慮:

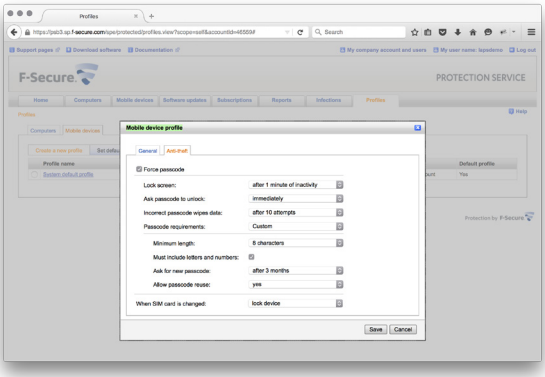
- 賬户登入管理
- 備份管理
- 防毒、補丁管理(Patch Management)
- 設備管理

## 賬户登入管理

首先，從個人方面說起。現在許多雲端應用服務已設有雙重身份認証功能，例如用户先按入登錄名稱(login name)及私人密碼(password)，服務端會向已登記的手機號碼以短訊形式(SMS)發放一個一次性使用的密碼(one-time password)，用户鍵入該密碼就可登入應用服務了。這個方法即使黑客在網絡上盜取了用户的密碼，亦不可能在線下(譬如透過手機網絡)看到你手機上的訊息，對用户取用賬户是一種雙重保障。另外，有些需要更高保密程度的應用如電子銀行(e-banking)，更須要使用由銀行發出的保安讀碼器(security token)作雙重身份認証。

關於密碼的强弱，應該以 8 位或以上數字、大小楷字母及符號組成。我們每人都有很多登入賬户，是否方便記憶而一律使用同一組密碼，或使用不同密碼組合以減少被入侵多個賬户的機會呢？我認為每人都可按自身的需要平衡兩方面。譬如，如經常在公眾網絡或別人設備進入賬户，那時眾多賬户使用同一組密碼是比較方便自己；如果是利用私人設備及瀏覽器使用雲端應用服務，以不同密碼登錄並採用瀏覽器默認密碼功能，也是一個好方法。另外，要登入賬户處理私隱、機密性較高的數據(如網上銀行、購物、公司重要檔案等)，在安全的、私人的網絡(如公司內聯網、家居網絡)上較可取。

對中小企業而言，在開通一種雲端應用服務時，應了解服務平台在啟動用户賬號(user account)及團體政策(group policy)有什麼保安設定可做，尤其是密碼管理方面，例如可否硬性執行每 3 個月要求用户更改密碼的政策。



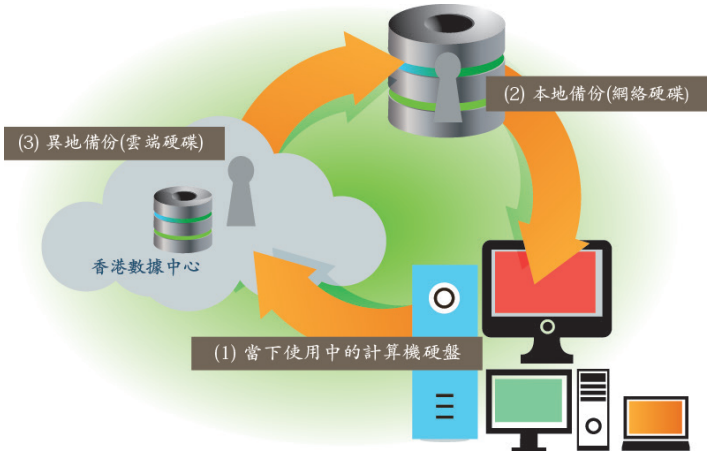

設定密碼的政策可利用雲端服務中心一併處理不同平台的計算機及智能設備 。

## 備份管理

雲端應用服務其中一項為人熟悉是雲端硬碟儲存服務(cloud storage)，用户可把檔案透過網絡傳送往雲端服務商的數據中心內的儲存硬體裡。對中小企業而言，雲端服務者相對專注而集中管理儲存系統，從而提供更穩定、安全及經濟的服務。以往中小企業，尤其是單一辦公室的商户，不可能像大企業做到異地備份(即把數據檔案儲存在不同辦公室地點)；今天，中小企業亦可透過以固定月費、按量繳費的雲端備份服務把重要的數據、檔案備份在雲端(即數據中心)。中小企業更可選擇應用有加密功能的雲端備份軟件，把加密了的數據及檔案放進雲端儲存中，即可完全避免有機會洩漏數據、檔案內容的機會。

過往，許多中小企業或會忽略備份管理，或者以今天非常經濟的硬體價錢及普及的雲端儲存服務，中小企業更值得花多點資源提昇這方面的資訊保安手段，避免因損失數據導致的經濟損失。

筆者建議可執行 3-2-1 備份策略: 把工作中的檔案(即當下使用在自己計算機設備)複製 2 份於不同的儲存位置(例如連接自己設備的另一個內置或外置硬碟、或內聯網絡上的儲存設備、即本地備份)，其中最少有 1 個複製檔案是在異地的雲端備份。




中小企業如何管理及執行多個用户端設備內的檔案備份亦非常重要。中小企業可選擇使用有雲端管理工具的雲端備份服務，透過網絡瀏覽器設定、管理及監督備份運作; 更可利用雲端恢復網頁，透過網絡服務恢復檔案在指定的用户端設備上。

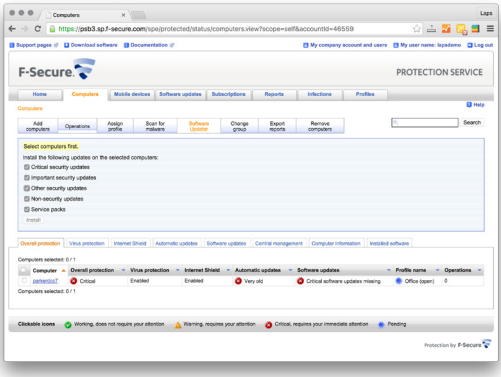
因連接互聯網絡的速度限制，今天雲端備份服務還是比較適合用於對中小企業重要而關鍵的檔案; 一些儲存量較大(如相片、影片)或長久不用的檔案可備份到本地備份的設備裡(local backup)。另外，假如萬一發生事故而需要恢復較多、較大容量的備份檔案，透過網絡下載十分需時; 建議中小企業可選擇在本地數據中心設置雲端備份儲存的服務商，如果服務能夠包含線下緊急數據恢復(offline disaster recovery)更佳(譬如，承諾可從數據中心直接下載恢復檔案到可攜帶式硬碟裡)。

## 防毒、補丁管理(Patch Management)

今天任何連接網絡上的設備、系統，包括種種不同的用户端設備都不可避免會受到黑客、病毒入侵的機會。現在甚至有許多叫“零日攻擊”(zero day attack)襲擊，即軟件保安機構或公司還來不及發現或製成防毒或解毒的編程碼(virus signature)，黑客或病毒已大肆侵襲網絡上的設備，令今天用户防不勝防。

中小企業要減低資訊保安事故發生的機會，第一道管理防線是必須保持系統更新，尤其是設備裡的作業系統(operating system)如:視窗(Windows)、Mac OS 及 iOS、Android 、Linux 等等。事實上許多黑客技術及軟件病毒能夠成功侵襲，都是建基於作業系統或應用軟件的程式碼缺陷(software bugs)和漏洞(vulnerabilities)而被製造出來的。所以軟件開發商會不斷更新程式碼以修補其錯誤; 這樣的過程過去 30 年計算機及資訊科技發展中少不了，未來雲端應用、互聯網服務亦無可避免。

堵塞軟件的缺陷和漏洞的執行對任何個人、公司非常重要，資訊科技界稱呼為補丁管理(patch management)。




利用雲端服務中心處理不同設備的補丁管理。

作業系統的補丁極重要，而且近年系統發展商如微軟、蘋果、谷歌的Windows、Mac OS、iOS、Android 差不多是數週一小更新(update)、數月大更新，以致一、兩年內必有系統提昇(upgrade)，用户應採用自動更新的策略，無論是使枱式或筆記型電腦、平板電腦或智能手機，應啟動自動更新及提示，一旦有系統更新及提昇，有必要盡快執行。事實上，微軟亦在推出Windows 10 裡强制一般用户的視窗執行自動更新保安檔案。還有，任何系統或軟件更新，謹記從軟件服務商官方網站下載安裝檔案。

今天的防毒軟件除適用於個人電腦、伺服器，更有版本可在平板電腦、智能手機安裝使用。防毒軟件不只能夠阻撓電腦病毒入侵，更包含其他功能如防止黑客網絡攻擊、私隱洩漏、偽冒網站過濾等，建議所有工作用途的平台應安裝第三方的防毒軟件。

現今流動工作普及，公司員工有機會利用流動工具如筆記型電腦、平板電腦或智能手機户外工作，僱主應該提供設有防毒、防網絡入侵的設備予員工工作; 防毒軟件服務就像一般軟件即服務，是按月、按量收費，中小企老闆可選擇訂閱合適數量的防毒軟件安裝在不同的流動設備上。防毒軟件服務供應商亦會提供易用的網頁介面讓企業可以一站式管理、監督各設備系統的安全狀態。

另外，BYOD(bring your own device)愈趨常見，員工有機會使用私自擁有的流動工具網上工作，僱主亦應考慮為員工訂閱防毒軟件，以減少企業發生資訊保安事故的機會。

近年來配有雲端監控的防毒軟件服務，用户端軟件除了可防毒、殺毒，亦設有雲端監視系統安全狀態，可遠端監察用户端作業系統更新狀況，雲端管理員並可按入遠端指令要求用户端作業系統執行軟件補丁及更新。

## 設備管理

除了作業系統軟件，應用軟件的程式安裝、更新及防毒管理亦不容忽視。中小企未必能夠像大企業般投入較大資源實施流動設備管理系統(MDM, mobile device management system)。從直接而簡單的運營考慮，建議中小企留意下列執行事宜:

1. 安排適合能力的員工或 IT 服務者以系統管理員人份(system administrator)安裝公司提供的應用軟件予公司設備上，不可容許員工私自更改公司設備設定。

2. 在日常工作，設備上的系統管理員人份不予使用。許多電腦病毒、黑客入侵都是從利用系統管理員權限作惡的。


3. 中小企業老闆或管理層應小心保管着系統管理員賬户的密碼，一旦資訊保安事故發生，或需要將賬户及密碼資料交予第三方服務者作緊急系統修復之用。密碼讓他人使用後應更改。

4. 任何應用軟件的全新安裝、更新或昇级，安裝程式或程式碼只有從軟件服務供應者的官方渠道獲取及下載; 尤其是供流動工具如 Apple iOS 、 Google Android 、Microsoft Windows，它們都有自己管理的應用程式店(app stores)，經官方網店發放的應用程式碼都經過審批、測試，使用起來比較安全; Android 設備上預設不允許店外下載程式碼的安裝，請長期啟動此設置，亦不應安裝不明來歷的應用程式安裝檔案(以 .apk 為檔案名字)。

5. 有些雲端應用軟件服務及流動設備用户端設置，授權應用軟件管理員可遠端搜尋設備位置(remote location)、遙控鎖機(remote lock)，甚至可遠端銷毀用户端硬體數據(remote wipe)，中小企業僱主如要在員工擁有的流動設備執行這些安全手段，請事先獲取員工同意及協議，以避免侵犯個人私隱或破壞他人資產。

6. 按雲端應用服務供應商的指示更新軟件程式碼 。

7. 在用户端設備上安裝及啟動防毒軟件。今天，即使是流動平板電腦、智能手機，亦應考慮安裝防毒軟件。

8. 避免使用不明的流動設備。市場上以 Android 為開放源碼作修改的流動設備廠商及品牌非常多，用户在選擇適合工作間使用的設備，可先多作資料搜集，例如參考公開的討論區信息，以便採購較安全、穩定的系統及設備。

# 第4章 雲端保安(應用服務篇)

## 4.1 雲端硬盤

一個適合中小企業使用的雲端應用服務是雲端硬盤(cloud drive)。雲端硬盤不單提供在線檔案儲存，更為團體工作提供一個可靠平台(collaboration); 員工不需再交換 “手指” 以傳遞數字檔案; 文件檔案設有不同版本記錄(versioning)，方便恢復及追查昔日的重要信息; 數據檔案的使用權限較容易統一管理。關於硬盤儲存使用，有以下建議:

計算機硬盤
- 儲存最近及常用的檔案。
- 經常清理一下，提高硬體效率、速度(例如使用 Apple Mac OS 系統裡 Disk Utility 提供的 First Aid 功能)。
- 把重要的目錄及檔案備份。
- 拷貝整個作業系統到一個外置儲存硬碟; 一旦計算機硬體出現甚麼毛病，亦可恢復計算機使用。例如在 Windows 10 可使用鏡碟 disk mirror 功能。

外置硬盤
- 儲存及備份了所有檔案，包括大容量的相片、視像檔案。
- 備份計算機系統儲存如用户設定、應用程式檔案。
- 最好把用户使用的檔案及系統使用的檔案分開不同硬體儲存。

雲端硬盤
- 可利用免费雲端硬盤服務如 iCloud、Dropbox 作少量儲存用途; 另外，附費服務功能較多，儲存量亦提高。
- 跟員工或外界分享檔案使用時注意權限的設定。
- 留意網絡一般上載速度較慢，要預留足夠時間上載大型文件如相片、視像檔案。

## 4.2 使用移動設備app的保安事項

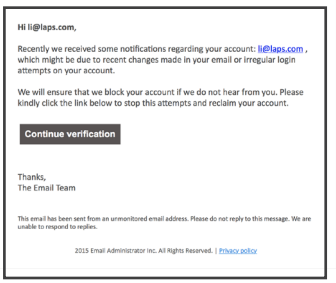
1. 從官方提供的渠道下載 app 安裝。
2. 在下載前，先參考官方店舖對 app 的說明，特別注意權限的設置; 小心一些 app 安裝後會授權獲取不必要的權限，譬如許多app都會不必要的存取、閱覽你的電話簿。
3. 在 Android 系統上，一般可往 Settings > Apps 查核已安裝 app 的權限設定; 遇上懷疑，先卸下(uninstall)該 app。
4. 在iOS系統上，利用 Settings > Privacy 可翻看每個 app 在使用你的聯絡人、位置、行事曆、相簿等等的狀態; 你可以逐一設置對其限制。


## 4.3 電郵

電郵可以說是第一代雲端服務。隨着流動設備普及，許多企業用家都以手機發送及閱覽電郵。電郵的運作可從個人設備(用户端)的軟件如視窗 Outlook、Outlook Express，透過網絡連接遠端電郵伺服器(即今天說的雲端部分)，交換登入信息後即可傳送電郵內容。

你可知道這樣的數據傳送過程也是否如利用 https:// 般加密的嗎? 如果是透過公眾 WiFi 網絡連線，也會把數據暴露了嗎? 請留意你的電郵系統是否使採用了 SSL/TLS 加密機制傳送電郵信息。

釣魚攻擊(phishing attack)是最常見的黑客襲擊。黑客會透過不同渠道，譬如社交網絡，收集關於你一個員工的資料，然後設計一個虛假電郵(fake email)，吸引你的員工按下電郵內附的一個虛假鏈結(fake weblink)，你的員工或許不察覺什麼便繼續工作; 其實鏈結是執行針對系統或軟件漏洞的黑客程式，在不知不覺間你的員工設備被入侵; 接着就是入侵內部網絡及伺服器。



這不是電影情節，2014 年一間非常知名的電子商貿網頁平台就是這樣被入侵，該網站隨後要求上千萬個平台用户更改密碼。

即使你安裝了最優秀的保安軟件或系統，亦未必能夠阻止零日攻擊，更何況你的設備或許還未更新或補丁; 警覺性高的用家才是你的最後防綫。

## 4.4 App stores 有許多免費的防病毒軟件可下載使用，可信嗎?

一般免費 app 會提供一個綜合的應用界面協助移動設備用家設置繁複的保安及私隱設置，還有機會包含清除不必要的記憶紀錄(clean cache)、優化記憶體運作(memory optimization)、甚至代理社交媒體賬户的私隱設定(例如 Facebook)等等。其實許多這些 app 處理的設置已分散在系統或應用程式的官方設置上，你應該考慮是否因安裝了這樣 app 會否授權第三者過多權限; 有許多免費軟件其實是臃腫軟件，內附更多第三方的網絡廣告或鏈結，即使排除保安考慮，額外的程式運作亦增加了使用設備資源的額外需求。選擇一些付費的、設有長期服務的防病毒實驗室的雲端保安服務較可取。

## 4.5 網絡交易要注意的事項

1. 必須使用官方網頁。其中一個最快捷及可靠的核實方法是從互聯網搜尋器調查一下。官方網址通常是最顯眼。
2. 確認在一個可信的網絡內瀏覽網頁。不建議使用公眾網絡; 手機移動上網較可取。
3. 盡量選擇第三方支付賬號付款方式，例如 PayPal、支付寶，避免在網絡上逮交信用咭及其他敏感資訊。不過，不應儲存太多現金於第三方支付賬號，它們跟傳統銀行在存款保障上或有不同。

4. 有雙重身份認証功能的話，應該啟用。
5. 不選擇由網頁記憶任何與繳付服務有關的密碼。
6. 若交易平台設有官方開發的手機程式，應先選擇使用。

## 4.6 瀏覽器保安事項

我們建議使用瀏覽器要注意下列事項:

1. 常見使用的瀏覽器有 Google Chrome, Mozilla Firefox, Microsoft Internet Explorer、Edge, Apple Safari，都設有防止自動彈出視窗功能，應開啟使用。
2. 瀏覽器服務配置有阻截虛假及問題網頁(fraudulent website warning)，可啟用其功能。
3. 在私隱設置裡選用 do not track request，以向網站或伺服器表示不希望瀏覽信息被紀錄; 不過，這個設定並不代表該網站或伺服器一定遵守。
4. 選擇不接收網頁廣告。
5. 避免安裝瀏覽器外掛程式如 Flash、Java Virtual Machine。新型的網頁服務已支援 HTML5 及 CSS3，適合普遍的多媒體、互動網頁的瀏覽。減少使用外掛瀏覽器的程式可減低暴露於程式漏洞的機會。
6. 要填寫敏感的資料如個人私隱、賬户密碼、表格等，必先確認瀏覽器是否已上鎖，即數據從用户端瀏覽器傳送到雲端伺服器是否加密的。
7. 在別人設備上使用瀏覽器應特別小心，不應選擇讓瀏覽器紀錄你的瀏覽信息及按入資料，並可在瀏覽器上開啟隱私瀏覽模式(incognito page); 完成瀏覽後可主動銷毀瀏覽紀錄。
8. 在瀏覽網頁時，尤其是需要填寫及發送任何重要資料，必先看清楚及確認網址 URL 是否正確; 遇有懷疑，可即時利用搜尋器核查網站地址或其內容真偽。

# 第5章 雲端保安(管理篇)

中小企業經常關注雲端服務是否安全，尤其是對於雲計算的隱私安全問題特別重視; 雲計算在信息安全方面，對中小企業一般來說有以下三種考慮:

- 在未經授權的情況下，他人以不正當的方式進行數據侵入，獲得用户數據
- 雲端服務供應商為獲取商業利益，未經授權下對用户信息進行收集和處理
- 手機應用程式有大量私隱訊息有機會被程式開發商收集及泄露

香港法例在個人及商業資訊保安方面算是完善。要讓服務及數據受本地法律保護，中小企業可考慮優先選用本地雲端應用服務。在選擇服務供應商方面，除了比較服務範圍、產品功用外，可對比跟雲端應用服務商訂定的服務水平協議(SLA，service level agreement)，並選擇服務水準協議與你的業務重要性相符的服務供應商。

服務水平協議是一合約協議。服務供應商會在協議內訂明服務水平、責任、優先事項，並就服務的可用性、成效和其他方面作出保證。有關協議是一項主要參考資料，可供用户比較和監察不同的雲端服務。服務水平協議內一般包括:

- 合約期限
- 服務終止、約滿安排，譬如: 承諾完約服務後若干日數銷毀儲存數據; 能否退回資料及數據
- 提早結束合約責任
- 保障私隱聲明
- 說明提供哪些保安功能或措施

對中小企業來說，客户服務及技術支援很重要。中小企業選擇服務商可考慮服務商是否有提供本地支援熱線(customer hotline)及上門支援(onsite support); 雲端應用服務優點是具彈性，服務商應可提供有限期的服務試用，並提供服務案例參考。

當你計劃推行雲端應用服務，周詳考慮的要點包括:

- 採取循序漸進，逐步實施策略
- 諮詢專家意見
- 選擇有經驗和技術的服務供應商，能夠提供雲端保安服務更佳
- 做好合約上和技術上的安排，以備未來需要轉用其他服務供應
- 可向本地服務商按雙方協議，要求提供服務終止將退回數據，並確保有關資料可供讀取和在需要時可復原

在確定業務需要和準備就緒採用雲端服務後，企業便可開始使用服務，營運一般包括以下各點:

- 與雲端服務供應商制訂合約安排，並簽訂雙方同意的服務水平協議
- 把現有系統內的應用程式資料、數據遷移
- 系統測試和驗收
- 系統啓用
- 用户培訓和支援
- 持續管理和監察服務表現

# 第6章 用家分享

## 中小企電子商貿信息安全技術與實踐 — Alibaba.com 案例

在本計劃課堂裡，我們邀請了多位嘉賓，分享了雲端應用服務信息保安的經驗及心得，令業界獲益良多。我們特別在此節錄與捷力亞洲企業有限公司(JSNA Asia Enterprises Limited)洪鎮峰先生(Mr. Anson Hung)的交流片段，了解洪鎮峰先生如何良好運作其阿里巴巴網上商鋪。

捷力亞洲企業有限公司(JSNA Asia Enterprises Limited)擁有超過十年豐富經驗，在內地自資設立工廠，專業生產各款保護拉伸膜及膠紙，主要在香港經營進出口批發工業包裝材料。捷力榮獲 Alibaba.com 香港2015傑出網商大賽的香港十大網商。

時間　：2015 年 7 月 30 日
地點　：職業訓練局高峰進修學院 灣仔活道27號 職業訓練局大樓
主持(D): 凌思商業方案 (Laps Solutions) 雲端服務經理、前香港阿里巴巴銷售主管 李松英先生
嘉賓(A): 捷力亞洲企業 (JSNA Asia Enterprises Limited) 洪鎮峰先生

D: Hi Anson，你利用 Alibaba.com 搵出口生意咁成功，好多謝你同各中小企老闆分享一下心得。電子商貿利用雲端互聯網服務，買賣雙方好似隔左一層屏障，誠信處理不容易，你係點樣去分辨買家優劣?

A: 首先，我們利用了平台提供的後台數據，並配合分析買家詢盤電郵。Alibaba.com 平台有一種叫買家數據行為的資訊，例如買家從哪個 IP address 使用平台，Alibaba.com 會記錄下來並提示我們它的對應國家; 當我從平台上查核買家自己報稱的國家，就能夠印証該買家是否偽冒。

D: 對，是很好的第一重防範偽冒。還有呢?

A: 現在雲端應用常說到大數據，Alibaba.com 有一項商業身份識別功能，買家過去在平台上的活動行為會被 Alibaba.com 數據模型驗證，並分成等級讓賣方參考。

D: 跟買家打交道有什麼可注意?

A: 劣質的、低潛質的買家一接觸我們賣家，通常不能夠提供足夠的產品查詢信息、會直接要求報價、又會先提出索取免費產品 sample; 看看買家的註冊年資也很重要。年資長的買家是假買家的機會相對較少。

D: 是否不是以公司電郵詢盤的買家就很可能是假?

A: 也不一定。如果是一個專業的買手，他需要每天處理大量查詢電郵; 為分流處理信息，會使用雲端上各種的電郵服務，譬如不同地區以不同免費電郵郵址作查詢，同時又可保障自己公司電郵免受垃圾電郵滋擾。所以我不會認定不使用公司電郵郵址就是假買家。相反，我經驗中這些詢盤亦成功做了不錯的生意。

D: 買賣是雙方面。你又怎樣在雲端網絡上表現為一個可信的賣方?

A: 實在可以有很多技考可做。首先，要善用產品照片。可放一些信息圍繞產品，例如背景是廠房、展覽室、放上生產認證 logo 等。

用户網站體驗也很重要。網站發放的資料不應太簡單，愈仔細愈好。自己公司網頁也不可以馬虎。今天買家多用平板電腦、智能手機瀏覽你的網頁，公司網頁應適用於各設備瀏覽。

另外，利用社交媒體把公司最新的產品、公司活動信息發佈，同時藉此與買家分享更多正確使用產品的方法，可建立專業形象，並多使用即時互動通訊跟買家溝通，務求盡快讓大家建立互信。

D: 我們常聽 O2O(Online to Offline)，線下你們又會做些什麼?

A: 我們會主動提供免費產品 sample，但不包運費。我們會為買家提供多種支付條件選擇: 線上有 PayPal，線下可用 T/T、直接銀行入數，甚至開信用証 L/C。

另外，每年我們仍會參加若干展覽會，讓潛在買家跟我們見面，以及歡迎潛在買家到公司參觀傾談。這樣的面對面的溝通，可以讓買家更了解我們公司文化及待客真誠，與線上銷售做到相輔相成的效果。

A: 好多謝 Anson 既經驗分享。

# 第7章 雲端保安服務例子

# Ahsay

| | |
|---|---|
| 公司名稱: | (中) 亞勢系統有限公司<br>(英) Ahsay Systems Corporation Limited |
| 服務名稱: | (中) Backup Solutions<br>(英) 備份軟件 |
| 電話: | +852 3580 8091 |
| 電郵: | sales-kb@ahsay.com |
| 網頁: | www.ahsay.com |

## 公司、機構簡介

Ahsay™ Systems Corporation 自 1999 年起一直專注研發數據備份技術，成為現時全球頂尖的 Backup Software 開發商之一。Ahsay™ 提供了全面及多元化的專業數據備份產品，能滿足企業的所有備份需求，在世界各地已有不少用戶安裝了Ahsay™ 的備份軟件，也有很多 IT 服務供應商採用了我們的產品以提供在線備份服務予他們的企業客戶。

背景

早在 1999 年，當寬頻仍未普及、大家仍是用 56k modem 上網的年代，Ahsay™ 看準寬頻上網必定成為大趨勢，而利用軟件透過網絡作備份勢必大行其道，所以決定開發企業級的備份軟件。今天，Ahsay™ 已經成為全球最受歡迎的企業備份軟件品牌之一。Ahsay™ 以香港為研發基地，成本遠較歐美對手為低，所以售價比其他歐美同類型軟件最少低 50%，我們的備份軟件功能齊備，真正切合企業需要，讓分銷商很容易便能打開各地的企業市場，所以大受市場歡迎。Ahsay™ 的軟件適合企業上下不同層面的用戶使用，加上產品經過嚴謹測試，技術相當穩定，所以大企業如香港的 NTT Com Asia 和韓國電訊公司 KTH 都選用 Ahsay™ 的產品。Ahsay™ Backup Software目前的版本支援達 32 種語言，覆蓋世界 90% 人口，成功打入各國市場。除主流的語言外，我們更支援較冷門的語言，如冰島語、捷克語、斯洛弗克語等，令我們的軟件能比其他對手更快滲透新的市場。

目標

為了實現「Backing up businesses, not just data.」這個目標，我們除了不斷的進行產品改進和增加與市場相關的備份功能，還同時重視合作夥伴的需求和市場發展趨勢，提供專業和及時的服務以及必要時候的增值專家服務。Ahsay™的優勢在於我們的創新理念及卓越的技術專長，這些競爭優勢可以使我們開發出更多的富有成本效益的業務解決方案。展望未來，我們將提供更多超值的在線遠程備份來滿足日常所需；將探索更多的商業機會，提供更多的創新產品、服務，讓更多的個人或企業受益於我們的備份軟件。

## 雲端服務說明

Ahsay™ 雲端數據保險庫乃安全可靠的異地網上備份服務，讓企業透過互聯網將 Microsoft Exchange Server、Microsoft SQL Server、Lotus Domino/Notes、Oracle database、MySQL database、Windows servers、Linux servers、桌面電腦和手提電腦的數據備份到 Ahsay™ 的數據中心，穩妥保護企業數據免遭意外而丟失。

### 一級本地數據中心 安全穩妥

Ahsay™ 高度安全的國際級數據中心已獲得 IT 服務管理標準 ISO20000 和 IT 安全管理標準 ISO27001 認證，使你重要的企業數據將獲得周全保護，確保你需要時能夠隨時還原檔案。

### 數據三重保密 絕對不會外洩

首先，備份帳戶具備密碼系統作保護，而數據會以用戶自訂的加密鑰匙以 256 位元作加密及壓縮，再以 128 位元 SSL 加密管道作傳輸，所以數據將獲得三重保護。加密鑰匙在備份過程中不會被傳送到備份伺服器上，即使是 Ahsay™ 的技術人員亦絕對無法開啟用戶所備份的檔案。

### 隨時隨地經 Internet 還原檔案

Ahsay™ 雲端數據保險庫讓用戶可以透過互聯網瀏覽器還原檔案，例如你在出差時突然需要從備份伺服器中提取某些已備份的檔案，你只需要登入自己的備份帳戶，並輸入自己的加密鑰匙，便可輕鬆地還原檔案，不受任何地域限制。

### 完全自動

初始化配置完成後，備份/複製會自動進行，無須人工干預，因此可以有效避免由人為失誤引起的數據丟失。

目標用戶

微型企業、小型企業 (主要)、中型企業 (主要)、大型企業


Ahsay™ 備份軟件具備 4 個核心備份程式：
AhsayOBM 和 AhsayACB 是客戶端備份程式，用作安裝在需要備份的伺服器、桌面電腦和手提電腦上。

AhsayOBS 是伺服器端程式，用作中央管理所有 AhsayOBM / AhsayACB 客戶端備份帳戶及儲存所有備份資料。

AhsayRPS 是複製伺服器程式，接近實時地接收由 AhsayOBS 複製出來的數據，提供多一重保障。

AhsayOBM 外掛備份模組
我們為 AhsayOBM 設計了不同的外掛備份模組，用作專業地備份虛擬機、數據庫、電郵系統、以及 Windows 系統，除了 VMware、Hyper-V 以及 Microsoft Exchange 個別郵箱備份模組外，其他模組都是隨 AhsayOBM 附送的。

# eBay

| | |
|---|---|
| 公司名稱: | eBay Inc. |
| 服務名稱: | eBay.com |
| 電話: | +852 3550 6042 |
| 網頁: | www.eBay.com.hk |

## 公司、機構簡介

eBay 香港致力協助本地賣家利用我們完善的電子商貿平台，將產品賣到全世界；並不時為賣家舉辦工作坊，介紹如何掌握網上創業及銷售技巧，傳授賺取豐富盈利的秘訣!

## 雲端服務說明

### ■ 1. 安全付款提示 ■

eBay 致力確保買家能在網絡市集中，擁有多種安全便利的付款選擇。正如 eBay 在安心購買指南中所強調的，我們非常鼓勵賣家提供 PayPal 這個付款方式，PayPal 不但使用方便，也採用了最先進的技術，能有效地保障買賣雙方，免受詐騙、退款或財務資料外洩等危險。擁有經銷商信用卡帳戶，或是使用合作夥伴程序處理付款的授權經銷商，也可以提供適當的選項，讓買家透過網絡或電話進行信用卡付款(可使用合作夥伴提供的結帳服務)。

注意：在多個較大規模的 eBay 市場，提供安全付款方式是增加買家對 eBay 市集信心的重要因素。PayPal 是 eBay 上最安全的付款方式之一，因此，有個別 eBay 網站可能要求把貨物賣到外國的賣家，把 PayPal 列作唯一的收款方式，而其他的收款方式可能不獲接納。請閱讀個別網站的刊登政策以獲取進一步資料。

新的付款服務不斷出現，eBay 會審慎評估這些新服務，檢驗他們的安全與

可靠性，以及是否適合網絡市集使用。一些不為 eBay 接納使用的付款服務可能在其他情況下能為顧客提供優良的服務。eBay 只是根據該些付款服務是否適合 eBay 網絡市集使用而作出評估。在評估時，eBay 主要會考慮以下因素：

- 付款模式能否確實保護買賣雙方的財務、個人資料，並提供良好的欺詐保護方案
- 付款模式是否周密，會否讓 eBay 會員產生任何疑慮，是否有任何可能遭人用來欺詐的漏洞
- 付款模式是否接受使用貴重金屬或其他非貨幣(例如：點數、里數、時數、優惠券、折扣)付款
- 付款服務是否具有長久而優良的歷史，能否提供長期的財務和銀行往來紀錄，證明自己為安全可靠的付款服務( eBay 通常不會接受無法提供過往紀錄的新興服務)
- 付款服務公司的履歷、背景以及其他投資事業
- 付款服務供應商在所在國家中，是否擁有適當的執照，是否符合當地法例要求

非電子付款方式通常不及網上付款便利，所能提供的保障亦較網上付款為低。不過，非電子付款方式亦可適用於某些類型的交易，如果賣家願意在刊登中接受此類付款方式，建議應採用最常使用的金融交易方式，例如：個人支票、銀行本票、匯票(請查閱下列例外例子)，或是貨到付款等等。

可在 eBay 香港使用的付款方式

賣家可以提供貨到付款或見面交收付款、PayPal、信用卡、個人支票、匯票(請查閱下列例外例子)或電匯方式。請注意，不是每種可在 eBay 香港使用的付款方式，都受到「eBay 標準買家購物安全保障方案」保障。

不可在 eBay 香港使用的付款方式

賣家不可慫恿買家以郵寄現金的方式付款。賣家不得勸誘買家利用現金立即轉帳服務(也就是不經由銀行，而是點對點式的現金轉帳)，例如以 Western Union / Moneygram 寄送現金。賣家也不可慫恿買家利用信用卡或提款卡，來支付款項。最後，賣家不可要求買家使用本政策中未明確許可的網上付款方式支付款項。

誤導及勸導買家不使用某些付款方式

如賣家在物品刊登中列明接受某些付款方式，他們絕不可選擇性提供這些已列出的付款方式，或勸導買家不要使用這些已列出的付款方式。

賣家一旦在「設定收款方式」一欄列出他們接受的付款方式後(包括 PayPal)，便要必定接受這些付款方式，也不可勸導買家不去使用這些付款方式。

此限制不限於物品刊登，乃包括所有買賣雙方有關於 eBay 交易的通訊。若違反此項政策規定，eBay 將按實際情況進行下列不同程度之處置：

- 取消刊登物品
- 限制帳戶使用權利
- 取消「超級賣家」資格(附註：適用於有「超級賣家」方案的 eBay 網站)
- 帳戶被凍結

## ■ 2. 檢舉假貨，提防受騙 ■

eBay 設立「保護知識產權方案」，是為了促進 eBay 及權益持有人之間的合作，以保障他們的知識產權。方案的主要內容包括：

- eBay 迅速移除超過 5,000 名知識產權持有人檢舉的拍賣物品。
- 每日主動監控並移除違反 eBay 防止刊登侵權物品政策的刊登物品。
- 可儲存搜尋結果，並透過最愛的關鍵字用電郵寄給用戶。
- 凍結一再違規的會員。
- 與版權持有人合作，尋找據稱侵權的會員個人資料。

無論如何，eBay 並不是 25,000 多種類別物品的相關知識產權專家，無法確認每日刊登在 eBay 上成千萬的物品是否侵權。所以，我們需要你的幫助以辨認並非一目了然的侵權物品。

## ■ 3. 提防私下交易 ■

在 eBay 以外的交易無法使用我們的功能和服務，包括我們的買家購物安全保障、信用評價、詢問會員的聯絡資料以及檢舉棄標物品及提出申訴的功能。

會員不得遊說他人在 eBay 以外購買或出售物品，進一步說明詳情，請參閱「提議在 eBay 以外私下進行交易」的政策。

### *如何辨別在 eBay 以外的交易*

要辨別你是否在 eBay 上交易的方式：
1. 前往「我的 eBay」，然後登入
2. 在頁面左方的「我要買的物品」下按一下「已買到的物品」
3. 找出你的購買物品及賣家的 eBay 會員帳號

如果你的「我的 eBay」並沒有該物品的紀錄，這有可能是在 eBay 網站以外進行的交易。

### *如何檢舉有欺詐嫌疑的交易*

如果你在 eBay 外私下交易購得或賣出物品，並認為受騙上當，可以向我們檢舉：
- 檢舉在 eBay 以外購買的物品
- 檢舉在 eBay 以外賣出的物品

我們亦鼓勵你採取以下行動：
- 聯絡當地執法機關
- 請向網絡欺詐投訴中心提出投訴
- 聯絡你使用的付款服務機構(如適用)
- 聯絡你的信用卡公司(如適用)。大多機構皆提供有網上交易保障，以保護被欺詐與收到不實物品的顧客
- 聯絡運送公司

## ■ 4. 了解你的交易夥伴 ■

信用指數是 eBay 社群一個重要部份。當你明白數字和星號背後的意義，你會更容易去評估其他會員的信譽。

## 信用指數及星號

信用指數是信用評價檔案最重要的內容之一，它是會員帳號旁括弧中的數字，你也可以在信用評價檔案上方看到此數字。你可能會在信用指數旁邊看到一個星號。

只要信用指數達到 10 或以上，便可獲得黃色的信用評價星星(  )。你收到的正面信用評級越多，信用指數便越高。星星的顏色亦會隨著信用指數的提升而改變，當指數超過 100,000 時，便可獲得最高等級的銀色流星(  )!

不同星號各有不同意義:

黃色之星 (  ) = 10 到 49 分

藍色之星 (  ) = 50 到 99 分

青綠色之星 (  ) = 100 到 499 分

紫色之星 (  ) = 500 到 999 分

紅色之星 (  ) = 1,000 到 4,999 分

綠色之星 (  ) = 5,000 到 9,999 分

黃色流星 (  ) = 10,000 到 24,999 分

青綠色流星 (  ) = 25,000 到 49,999 分

紫色流星 (  ) = 50,000 到 99,999 分

紅色流星 (  ) = 100,000 分或至 499,999 分

綠色流星 (  ) = 500,000 分或至 999,999 分

銀色流星 (  ) = 1,000,000 分或以上

# F-Secure

| | |
|---|---|
| 公司名稱: | F-Secure |
| 服務名稱: | F-Secure.com |
| 網頁: | www.f-secure.com |

公司、機構簡介

總部設於芬蘭的 F-Secure 於 1988 年成立，26 年來不斷為資訊保安研究發展。全球設有 25 間辦公室, 支援 100 多個國家，亞洲區總部設於馬來西亞吉隆坡, 提供技術支援，產品研發等等。透過超過 200 間電訊營運商及 3500 間合作伙伴，為數以百萬計各樣用戶提供資訊保安方案。連續4年(2011-2014)，得非牟利組織 AV-Test.org 評選為“最佳保護”。總部每日分析及處理二十五萬個可疑樣本，以及二百五十億個網址測試, 確保用戶上網安全。F-Secure 產品覆蓋個人客戶，中小企以致誇國大型企業。

## 12 招確保中小型企業有關計算機保安的手段

跟據工業貿易署資料，香港約有 32 萬家中小企業，佔全港企業總數逾百份之九十八，合共聘用了約五成的私營機構僱員。現在想像你是一個網絡犯罪者，正挑選你下一個網絡攻擊目標；你會去選擇一批擁有巨額資金的中小企業，它們缺乏安全控制，或去選擇大型企業，而它們內部有側重於保護公司資產的安全團隊? 這不像電影: 黑客不希望是一個挑戰，他們要的是錢，會捨難取易。

無論你是否內部擁有一支 IT 團隊或使用外判服務商的支持，以下是保護你公司的一些提示:

1. 立即補丁 (patching)
當系統製造商發現一個軟件漏洞，他們會修補這個問題，並向所有註冊用户發出修正 (fixes)，這就是經常彈出屏幕上的軟件更新指示。一些企業依靠員工自行執行升級，而有些則集中管理。無論哪種方式，應立即修補。已發佈的安全漏洞是黑客們會知道存在的安全漏洞，同時他們也知道，數以百萬計的用户不會刻意去修補它們。除非你為電腦打了補丁，否則你很容易受到安全威脅。

2. 盡快將 Windows XP 升級
2015年4月，微軟停止對 Windows XP 的軟件支持。這意味著，與操作系統的任何漏洞將不被修補。黑客只要找到這些故障，便可以利用它們植入惡意軟件並進入你的計算機及網絡。避免成為受害者的唯一辦法是為你的操作系統升級。Windows XP 後推出的操作系統在設計時以安全為優先，因此是較好的選擇。

3. 手機和平板電腦需要保護
要保護計算機網絡，更要保護連接到它的移動設備。移動設備會被利用成為網絡犯罪的接入點。如果一個黑客入侵了你的工作電話，他有機會獲得你的聯繫人、電子郵件或財務信息，更不用說網絡數據。無論你的員工在使用公司提供的或個人的移動設備，它們都必須安全地運作。

4. 備份
近年勒索攻擊 (ransomware) 接連發生，趨勢變得普遍。你一旦遭到攻擊，將會在你的設備屏幕上出現一條消息，告訴你你的文件或電腦已被加密、上鎖，它會要求贖金你才能夠再次使用數據或設備。當然，即使你繳付了贖金，也不能保證你會得到問題解決。你若有設置自動備份，即使發生這樣的攻擊，你也不會失去你的數據內容。但要注意，離線備份是必須的，但勒索攻擊亦可能把你的備份檔案加密。

5. 使用更新的防病毒軟件
防病毒軟件運作像一個社區。當檢測到一個新的惡意軟件試圖侵略計算機或移動裝置，它會被隔離 (quarantined) 並發送至防病毒實驗室進行測試和解毒。一旦病毒的簽名 (virus signature) 確定，病毒簽名會被發送到實驗室的每個註冊用户的防病毒軟件裡，以保護計算機或移動裝置免受威脅。這過程可以在短短的 8 秒發生！如果沒有最新的殺毒軟件，你沒有這種保護。在撰寫本文的時候，我們的實驗室 (F-Secure Labs) 在過去的 24 小時已經檢測到 15,742 件惡意軟件及其變種檔案。

6. 確保你的雲端和虛擬環境也安全
雲端服務和虛擬化技術越來越普遍，為中小型企業所採用，以提高性能及降低IT運營成本。你可以想像，確保這些環境安全也很重要，以防止你公司的信息受到不必要的窺探。

7. 給員工使用隱私屏幕 (privacy filter)
隱私屏幕夾在一台筆記本電腦屏幕或移動設備上。設備的用户不會注意到屏幕上任何區別，但是在他們旁邊的人卻看不到任何東西，只是一個黑色的屏幕。對於經常户外及流動工作、出差工幹人仕十分重要。

8. 保護你的無線網絡
無線網絡為企業普遍使用超過 10 年，令人驚訝的是很多網絡依然不安全。此外，應該最少使用 WPA2 (WiFi Protected Access 2) 加密，而不是 WEP (Wired Equivalent Privacy)。WEP 是比較容易被黑客破解；或者選擇使用以增加安全性的VPN服務更佳。

9. 密碼
“password”已不再是最常用的密碼。不幸的是，它被“123456”取代。黑客利用工具嘗試多種組合來破解密碼，最常見的如“123456”必然是最先嘗試。之後，他們嘗試從文字的組合，或從網上尋找受攻擊目標者的信息及線索(譬如生日期)，以破解密碼。密碼內添加符號和數字可使更難破解。

10. 你的數據對別人是比你自己認為更有趣
經常會有中小企業認為他們的數據是不會吸引任何人，所以就沒有必要進行保護。但你的競爭對手在意它，因為這意味著他們將能夠找尋削弱你生意、競爭力的機會。你應在乎或需要向網絡犯罪支付贖金。永遠不要低估你的資訊對別人的價值。

11. 員工
當涉及到信息安全，員工往往是最薄弱的環節，所以應時時提醒他們資訊保安的重要。建立他們可執行的、確保公司安全運作和你對他們期望的安全法則。經常在會議上提點資訊保安對公司及個人的重要性。

12. 設備會丟失或被盜
失物及被盜或會發生，所以最好準備如何應對。最近，我在斯德哥爾摩一家酒吧丟失了我的電話。我遠程使用運行在手機上的安全軟件抹去所有數據。第二天，我更換了手機，並立即上傳我在雲端備份所有的聯繫人和數據。失去的設備是不可避免的，但失去的時間和內容是完全可以避免。

<< 本文由 F-Secure Hong Kong 提供 >>


# HPE

| | |
|---|---|
| 公司名稱: | (中) 惠普企業<br>(英) Hewlett Packward Enterprise |
| 服務名稱: | 雲端數據安全解決方案 |
| 電郵: | hpswmktghk@hpe.com |
| 網頁: | http://www.hpe.com/us/en/solutions/security.html |
| 聯絡人: | HPE 軟件部市務部 |

## 公司、機構簡介

惠普作為企業安全解決方案供應商的領導者，為現代企業處於複雜及多變 IT 環境提供最佳的解決方案，以防禦最新的網絡系統威脅。整合了 ArcSight、Fortify 和 Atalla Voltage 等市場領先產品的惠普安全智慧及風險管理平台 (SIRM - Security Intelligence and Risk Management) 獨家提供先進的安全事件關聯分析、應用程式保護和網絡防護, 以保護當今的應用程式和 IT 基礎設施免遭複雜的網絡攻擊的威脅。欲了解更多詳情，請瀏覽: http://www.hpe.com/us/en/solutions/security.html 。

## 雲端服務說明

隨著流動商務普及，由SaaS (軟件即服務)開創的雲端工作時代已經來臨。今天從事各行各業的中小企，已廣泛使用雲端應用來處理日常工作，不但可以提供團隊協作能力、省去日常 IT 維護及軟件管理工作，同時降低軟硬件購置成本，迅速提升生產力。

不過，對中小企而言，雲端應用有利也有弊，最容易忽略的就是資訊安全方面。由於雲端應用的存取方式無處不在，容易導致敏感資料存留在各種雲端應用內，瞬間就會外流或被分享出外。一旦商業機密或客戶資料外洩，引起

法律訴訟風險，會對中小企營運造成致命打擊。面對 SaaS 工作模式帶來一系列資訊安全及營運風險，加上中小企缺乏 IT 保安方面專才，這時便需要一種嶄新、簡易的方法為雲端應用進行數據監管、風險管理和網絡安全保護。

## 認清您的雲服務

在選擇合適的雲安全服務前，首先要注意您所選用的雲服務會否涉及哪些保安風險。綜觀市場上中小企常用的雲服務，主要有Google Apps、Microsoft Office 365、Dropbox 及 Salesforce。有三大使用特徵與企業安全風險息息相關。

1. 隨時隨地任何設備。用戶的帳戶和密碼可以從 SaaS 應用於任何設備、地方及時間存取，這包括通過託管和非託管的設備來存取。這跟傳統內部部署應用通過企業 VPN 網絡及指定設備等高度安全機制不同，容易內附有害程式而竊取資料。
2. 用戶定義使用方式。雲端應用是由用戶，不是由 IT 部門來定義那些信息(文件或文件夾)可使用和共享服務，如 Dropbox、Office 365 或 Google Apps。用戶可以邀請協作者，並與指定某人共享這些文件。由於這些用戶大多不是 IT 專才，不會理解分享文件過程中可能招致企業安全風險。
3. 專屬的數據共享功能。雲應用有千萬種數據共享和儲存方式，每一個 SaaS 應用程式各有不同。例如，Salesforce 的企業數據可能會存留在聊天文檔(Chatter files)內，現有防火牆和入侵防禦系統未必能透視 SaaS 應用中的數據，或不明白每一個 SaaS 應用交易的細微之處。

因此，選擇雲安全解決方案必須能夠識別雲應用內的數據，並了解與用戶相關的互動情況。例如，存有哪些數據？誰與它互動？執行哪些事務？數據如何被存取和共享？以及哪些類型的數據必須滿足法規要求？這些範疇均屬於雲服務可直接影響中小企營運風險。

## 監管一切雲端應用

中小企總希望將資訊安全置於內部 IT 可以控制的環境內，他們需要在不犧牲工作效率及使用體驗下，達致安全監管及保護各式各樣雲端應用，主要有三項原則：

高透明度：能在多個雲應用上獲取對每個用戶交互的深入了解，實現完整的審計跟蹤功能。簡易探索內部和外部協作者的數據共享活動。

簡易監管：監管相應雲應用策略，包括數據共享、應用使用和訪問控制策略以及探索第三方應用程式功能。可根據雲應用日誌創建具體策略和報告。

加強保護：檢測及禁止雲服務內的高風險使用情況、異常行為和安全事件。

## HPE 雲訪問安全保護平台

HPE 雲訪問安全保護平台(HPE Cloud Access Security Protection Platform)是最佳解決方案，能確保雲資源被訪問及存取時能有效執行企業安全策略，這些策略包括安全認證、登錄、授權、用戶憑據、設備配置管理、檔案加密、日誌、警告和惡意代碼檢測防護等功能。

HPE 雲訪問安全保護平台設有 Adallom 雲訪問安全代理解決方案，可與您的雲應用無縫整合，不會影響最終用戶的使用體驗。Adallom 提供的 SaaS 安全架構已證實能有效保護企業免受黑客攻擊，包括瞄準 Salesforce.com 的 Zeus 惡意軟件變種，以及針對 Office 365 的漏洞。有了這款解決方案，您可以隨時隨地在任何設備上查看、監管和保護數據。同時，提供全面的審計跟蹤功能，可將每項活動與用戶關聯起來，讓您可以監管雲應用的使用、保護企業數據，並在帳戶被盜或出現危險行為時及時採取應對措施。

## 使用模式按您所需

在實施方面非常容易，Adallom 雲訪問安全代理解決方案易於運行在任何用戶、網絡及設備上，不用修改網絡配置或安裝終端代理，主要有三種使用模式：

應用程式介面(API)模式 - 直接整合雲應用的 API，達到快速設置的優點。該 API 模式允許收集和分析用戶身份和活動信息的相關性，如登錄/註銷、地點、時間、上傳、下載，共享權限和橫跨多個雲應用。一旦與多個雲應用集成，Adallom 能分析來自不同數據源的信息，並創建一個指揮和控制中心(Adallom 控制台)，提供企業內 SaaS 活動的全面可視性，滿足雲監管和法規遵從需求。

Adallom SmartProxy 模式 - 所有應用流量均通過 Adallom 雲服務，能為您提供完整的雲應用使用的透明度和實時控制用戶的請求、廠商回應及來自託管或非託管裝置的活動。該 Adallom SmartProxy 技術提供實時警報和阻斷一切違規活動，更提供即時控制存取敏感訊息，包括地理信息，設備資料和數據。

混合模式 - 結合了 API 和 Adallom SmartProxy 模式的好處，滿足監控各式各樣雲應用的使用情況。例如，API 模式針對正常訪問，而 Adallom

SmartProxy 專為非託管設備的訪問而設。一旦部署，Adallom 會不斷收集用戶的身份和活動信息，加上 Adallom SmartEngine 啟發式技術能深入了解每個用戶的使用行為，當用戶行為偏離正常表現時，系統會立即提供警示。

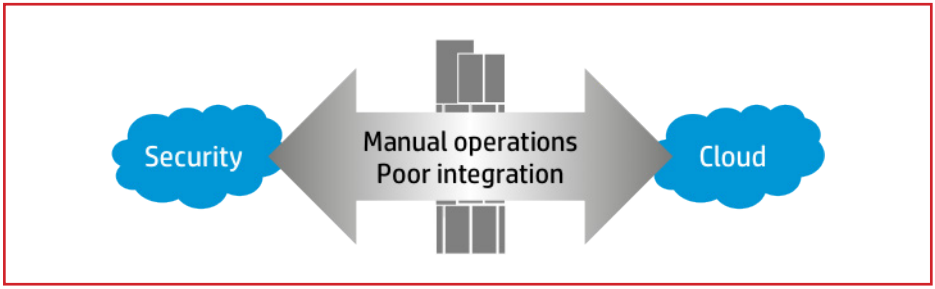
解決方案: HPE 雲保護平台

可用於 SaaS 模式、內部部署或私有雲部署。
使用權以每個平台的用戶及每個應用的用戶計算。

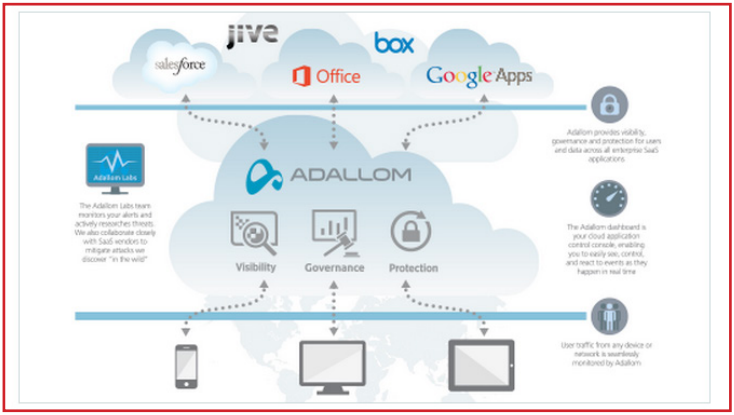
雲安全刻不容緩

商業競爭不斷加劇，如果我們要在數碼新經濟模式中突圍而出，必須大量使用 SaaS 模式的雲端應用來提升整體競爭力。每個存留在雲內的數據均是企業寶貴資產，為免夜長夢多，企業必須積極部署高透明度、嚴格監管和保護所有雲應用的雲安全服務，至關重要。

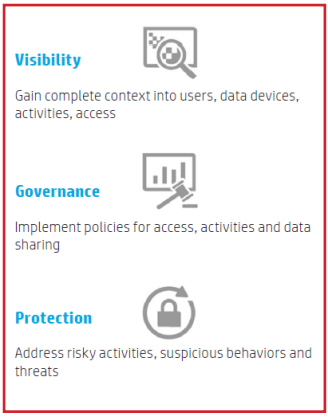
URL 或其他參考資訊網上地址
http://www8.hp.com/us/en/software-solutions/cloud-data-security-governance




傳統網絡安全模式與雲服務未能有效整合，中小企只能以有限的人手操作進行安全監控。




Adallom 雲訪問安全代理解決方案已證實能有效保護企業免受黑客攻擊，包括瞄準 Salesforce.com 的 Zeus 惡意軟件變種，以及針對 Office 365 的漏洞。




中小企總希望將資訊安全置於內部 IT 可以控制範圍之內，他們需要針對所有雲應用提供高透明度、簡易監管及加強保護的功能。

# Laps

| | |
|---|---|
| 公司名稱: | (中) 凌思商業方案有限公司<br>(英) Laps Solutions Limited |
| 服務名稱: | (中) 雲計算應用 . 服務卓越<br>(英) cloud solutions . service excellence |
| 電話: | +852 6297 5639 |
| 電郵: | cs@laps.hk |
| 網頁: | www.lapssolutions.com |
| 聯絡人: | Customer Service |
| 社交媒體聯絡: | www.facebook.com/LapsSolutions |

## 公司、機構簡介

凌思方案提供互聯網、移動網络上一站式、可靠、安全的雲計算服務。為企業客戶提供網絡和伺服器託管服務、應用軟件開發和解決方案。我們目標是幫助客戶輕易地使用雲計算和在線服務，讓他們能夠專注於自己的核心業務。

## 雲端服務說明

創意及編程服務 (LCCB，Laps Creative & Coding for Business)

- 我們並非傳統的應用程式開發公司，我們致力兼顧良好的技術功能、高質素的版面設計和實際的用戶需要。我們相信只有一個易於使用的、有吸引力的和高效率的應用程式，才能為客戶的業務帶來效益和利潤
- 在 Web 和移動應用開發項目中，我們採用回應式網頁設計，建立能與桌面電腦、智能手機和平板電腦進行良好互動的網頁設計，令瀏覽者得到優質的用家體驗

企業級跨平台、跨裝置保安服務 (LPSB，Laps Protection Service for Business)

- 免費上門安裝、設置掃毒軟件及進行預防性病毒掃描、清除病毒服務
- 使用屢獲殊榮、以芬蘭為基地的 F-Secure 安全軟件及解決方案
- 保護 PC、伺服務、Mac、平板電腦及手機免受病毒或網絡安全威脅
- 單一雲端控制平台以管理多台網絡設備

保安心雲備份服務 (LCBB，Laps Cloud Backup for Business)

- 免費上門安裝及設置備份軟件服務
- 檔案、數據傳輸及儲存百分百加密保護
- 檔案、數據保存於香港數據中心，受香港法律保障

凌雲陣 (LCSB，Laps Cloudsite Service for Business)

- 凌思是你推行雲計算應用的理想合作夥伴。我們提供完整和成熟的雲計算組合，包括私有雲、混合雲到公有雲
- 我們的「凌雲陣」Laps Cloudsite 服務目前提供在線訂閱和管理伺服器託管服務的面板，服務種類包括: 雲端伺服器及寄存服務 (Cloud Hosting for Busines)、虛擬專用伺服器 (VPS) 和雲基建 (Cloud Infrastructure)，並有多種服務計劃可供選擇

我們承諾認真幫助處理你的查詢。我們有專業和充份了解我們產品和服務的團隊解答你的疑難。凌雲台 (Laps Helpdesk) 有多樣方式讓你可以聯絡我們，我們希望有最快捷的方式跟你連繫。

# Readyspace

| | |
|---|---|
| 公司名稱: | (中) 銳空科技有限公司<br>(英) ReadySpace Limited |
| 服務名稱: | (中) 雲端服務<br>(英) Cloud Service |
| 電話: | 3568 3372 |
| 電郵: | info@readyspace.com.hk |
| 網頁: | www.readyspace.com.hk |
| 聯絡人: | 蕭先生 |

## 公司、機構簡介

ReadySpace 是一間 IT 寄存網路服務供應商，辦事處設於新加坡、香港、中國、菲律賓、馬來西亞及美國，提供範圍廣泛的雲端基礎設施服務 (Iaas) 給與世界各地不同類型和大小規模的企業。其服務包括雲端寄存、雲端伺服器、專屬伺服器、雲端基礎建設服務、託管微軟Exchange Server 伺服器、電郵保安等等。ReadySpace 提供具競爭力的價格與業內頂尖的服務和支援水平，其最與眾不同之處是不斷改善本身的服務質素，並還提供最新的技術給客戶，一如 ReadySpace 的名字，給予客戶業務成長的空間。

ReadySpace 在其先進的數據中心內部署其運作，其數據中心是在亞太區其中最大的設施之一。為達到無可取替的服務多樣性、靈活性和可靠性，ReadySpace 的網路中立數據中心及服務透過直接互連至最大的聚合網路 Equinix 數據中心，來克服其他現有的數據中心、網路和互聯網業務的限制。其數據中心獲得 SunTone 認證，意味著數據中心基礎設施、運營實踐、硬體、軟體和整體提供的服務，符合所需的高品質服務部署和嚴格標準。

## 雲端服務說明

ISO 27001, MTCS Implementation
訪問控制平台管理，認證實踐
多重雲端安全標準

數據保護
R1Soft CDP, Symantec Enterprise, BackupAgent

網絡保護
Fortigate – VPN, IPS, SSL Certificates

數據完整性
Guardtime

外部安全掃描
StopTheHacker – Vulnerability Assessment, Malware Protection
Trustwave – PCI Compliance Assessment
F-Secure Security

對外安全性
Infotect – iNSIGHT for Web Server (IWS), 防止信息洩露

# TGT

| | |
|---|---|
| 公司名稱: | (中) 名氣通電訊有限公司<br>(英) Towngas Telecommunications Company Limited |
| 服務名稱: | (中) ACT 雲端服務<br>(英) ACT Cloud Service |
| 電話: | 2963 3666 |
| 電郵: | info@towngastelecom.com |
| 網頁: | http://towngastelecom.com<br>http://www.tgtact.com |
| 聯絡人: | Mandy Lin |
| 社交媒體聯絡: | Facebook: Towngas Telecom TGT 名氣通電訊 |

## 公司、機構簡介

名氣通電訊有限公司(名氣通)為香港中華煤氣有限公司(煤氣公司)的全資附屬機構，於 2004 年正式成立，主要業務包括網絡構建、數據中心與智能家居及雲計算服務。秉承煤氣公司的優良服務文化，名氣通作為中立電訊供應商，在香港及內地均擁有多個世界級數據中心及網路基建服務，並利用煤氣管道光纖技術於香港鋪設光纖網路，為各大企業、國際網路服務商及專業客戶提供更廣泛的服務。

## 雲端服務說明

名氣通為阿里雲進軍海外市場的重要合作夥伴，共同策劃及結合雙方的營運優勢及商務模式，攜手為企業提供服務範圍更廣闊，運算資源更靈活的雲端服務。

新一代的雲端服務 ACT，提供即時、靈活、低成本及安全可靠的 IT 資料，給信心予本港、中國大陸及其他海外的企業，促進其業務增長。ACT 雲端服務有四种產品，包括彈性運算服務、伺服器負載平衡系統、關係型數據庫服務及開放式存儲服務。

## 目標用戶

本港、中國大陸及其他海外的企業

# Trendmicro

| | |
|---|---|
| 公司名稱: | (中) 趨勢科技<br>(英) Trend Micro |
| 服務名稱: | (中) 雲端保安<br>(英) Cloud Security |
| 電話: | 2866 4362 |
| 電郵: | tmhk@trendmicro.com.hk |
| 網頁: | http://trendmicro.com.hk |
| 聯絡人: | Claudius Lam |

## 公司、機構簡介

趨勢科技為資訊安全軟件全球領導廠商，致力創造一個安全的資訊交換世界。憑著 26 年的經驗，我們的解決方案能為消費者、企業及政府機構提供多層式資料安全防護，涵蓋行動裝置、端點、閘道、伺服器以及雲端。趨勢科技是智慧型資訊防護的動力，擁有創新的防護技術，不僅容易部署與管理，而且更能隨著不斷變化的生態體系而演進。我們所有解決方案皆以趨勢科技 Smart Protection Network™ 雲端基礎架構的全球威脅情報為後盾，更有全球 1,200 多位威脅專家在背後支援。如需更多資訊，請至：http://trendmicro.hk。

## 雲端服務說明

趨勢科技 Deep Security 結合了入侵偵測及防禦、防火牆、一致性監控、記錄檔檢查等能力，可為動態數據中心的實體、虛擬或雲端伺服器提供進階防護。

Deep Security 能保護機密資料與重要應用程式，協助預防資料竄改，確保企業永續營運，並且讓企業遵循重要的標準與法規，例如：PCI、FISMA 與 HIPAA。這套解決方案讓企業發掘可疑的活動和行為，主動採取預防措施來確保資料中心安全。

其獨特防護範圍包括入侵偵測及防禦、網站應用程式防護、網絡應用程式控管、防火牆、完整性監控及紀錄檔檢查等。

另一方面，Deep Security 也透過服務方式為使用公有雲(如 Amazon Web Services、Microsoft Azure 及 VMware vCloud)的用戶提供全面的安全防護功能，包括：

- 入侵偵測及防護 - 利用自動更新的保安政策來防止未修補的漏洞遭到攻擊，確保雲端伺服器在適當的時間獲得適當的防護。
- 進階防火牆 - 在每台雲端伺服器的周邊築起一道防火牆以防範攻擊，將通訊局限於絕對必要的連接埠和通訊協定。
- 惡意程式防護 - 每一天每一秒鐘都有新的惡意程式出現，Deep Security as a Service 能提供即時防護，防止一重重專門攻擊系統和竊取資料的惡意程式。
- 完整性監控 - 符合檔案及系統監控方面的遵規要求，確保偵測並通報未經授權或不合政策的變更。
- 記錄檔檢查 - 識別隱藏在多筆記錄內的重要保安事故，將可疑事件傳送到 SIEM 系統或是中央記錄伺服器，在此進行關聯分析、報表與歸檔。
- 網站信譽評級 - 控管伺服器通訊對象所在的網域，降低遭入侵的風險。

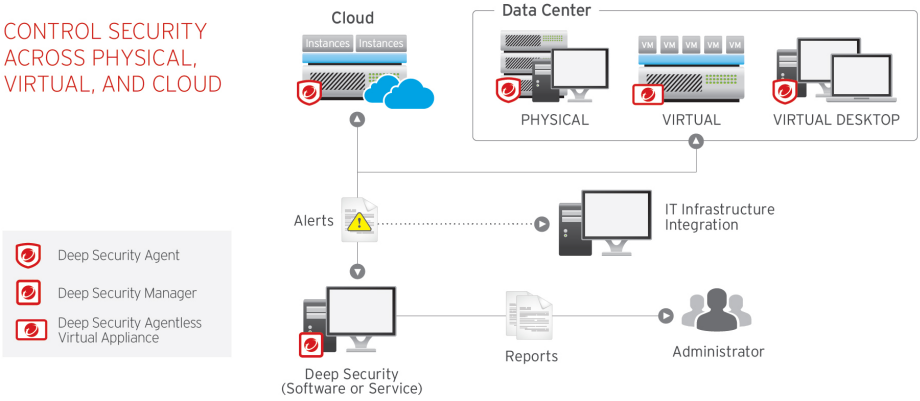
Deep Security as a Service 採用可從集中管理主控台快速彈性部署的服務模式，讓用戶迅速而輕鬆地為雲端工作負載加強安全防護。

### 目標用戶

跨行業用戶無論規模大小均可採用 Trend Micro Deep Security 雲端防護方案

## 其他參考資訊網上地址

跨行業用戶無論規模大小均可採用 Trend Micro Deep Security 雲端防護方案
http://www.trendmicro.com.hk/en-hk/enterprise/cloud-solutions/deep-security/index.html



# 聯絡

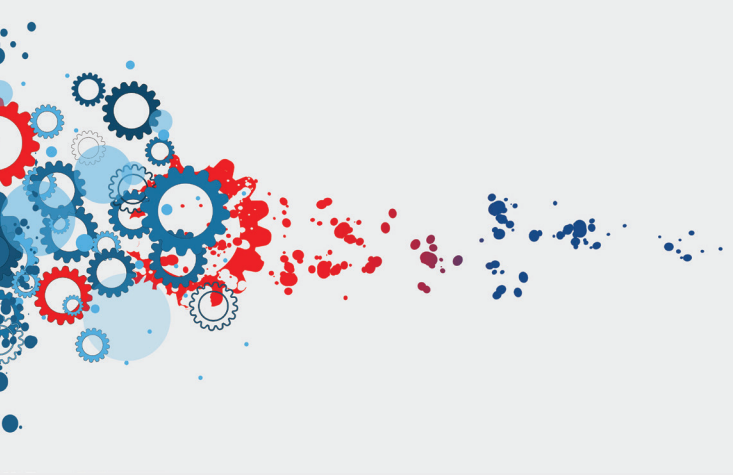
「提升香港中小企在資訊科技及雲端商用上的安全策略」

香港中小型企業總商會
The Hong Kong General Chamber of Small and Medium Business
通訊地址：九龍紅磡民裕街41號凱旋工商中心第一期11字樓D室
電話：(852) 2325 9189
傳真：(852) 2329 3749
電郵：info@hkgcsmb.org.hk

職業訓練局高峰進修學院
PEAK of Vocational Training Council
通訊地址：香港灣仔活道27號 職業訓練局大樓9樓
電話：(852) 2919 1429
傳真：(852) 2891 5707
電郵：kento1991@vtc.edu.hk

香港軟件行業協會(Hong Kong Software Industry Association)
通訊地址：新界葵涌葵昌路29號東海大廈A座4樓
電話：(852) 3913 2000
傳真：(852) 3011 3073
電郵：info@hksia.hk

免費諮詢服務、協助中小企業應用雲端服務
電郵：cloud4sme@gmail.com
項目網址：http://cloud4smb.hk



# SME Cloud Security

## 中小企雲端服務信息安全

合作/支持機構：（排名不分先後）