Global Headquarters:5 Speen Street Framingham,MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

# IDC白皮書

## 企業安全防護：化繁為簡的智慧方案

Sponsored by : Trend Micro

作者：Charles J. Kolodgy Andrew Hanson
2009年2月

## IDC的觀點

“時間就是金錢”和“知識就是力量”可謂老生常談，但是對於內容安全專業人員而言，它們卻依然具有實實在在的意義。內容安全威脅不斷增加，而攻擊者則憑藉更加複雜而且不斷變化的攻擊形式圍攻企業。這些威脅的提交速度甚至給安全專業人員都施加了更大的壓力。

對於精明的攻擊者，傳統的安全方法不再具有能夠保持優勢的強大功能。主要依賴病毒碼的解決方案必須部署在企業的所有用戶端和伺服器上，這將導致保護延遲。而且病毒碼因為變種病毒數量的增加而變得越來越大，佔用了更多的額外資源。隨著網路威脅的不斷增加，這個問題將變得愈來愈嚴重。

很多企業都在投資購買各種Endpoint安全產品。但是這種Endpoint端點類產品不但沒有解決安全問題，反而增加了新的代價--更加繁複的工作--不斷的部署和更新、監測和管理以及不間斷的支持要求等。這種情況下，時間就是金錢，企業花費了數十億美元打造了堅固的防禦體系，但是複雜的管理方式卻迫使企業面臨超出原本需要解決的問題範疇內的的更多額外的問題。

解決這一問題仍然需要一種全新的且具有創新意義方法，即能夠提供及時保護，同時降低複雜性。

對於內容安全，知識就是為那些能夠迅速識別並攔截網頁威脅的創新方法和解決方案提供力量的堅實基礎。趨勢科技充分瞭解對於即時性的要求，知曉攻擊所採用的各種方法。基於這種思想，趨勢科技開發了一種全新的安全方法，採用雲安全用戶端架構作為其解決方案的基礎，為安全專業人員奪回了優勢。

## 方法

IDC採訪了眾多行業公司的高級管理人員，以便明確客戶和市場對於安全解決方案發展趨勢的看法。此外，IDC還會見了趨勢科技的管理團隊，審核該公司用來解決客戶安全挑戰的全新方法。本白皮書使用了所有這些研究視點，力圖建立對企業所面臨的內容安全問題的真實看法，闡述趨勢科技的全新方法如何能夠提供解決之道。

# 情況概覽

## IT安全的紛雜世界

### *網路威脅*

IDC研究顯示，惡意程式（病毒、特洛伊、蠕蟲、間諜軟體等）仍然是最為嚴重的威脅，對企業的影響最大。每天都有數千種新型惡意程式變種產生，而IT工作人員則努力與各種新型攻擊保持同步，以防止其造成巨大破壞。現在病毒感染的速度以小時和分鐘而非星期和天數計量。最危險的惡意程式形式之一就是間諜軟體。IDC認為，幾乎有四分之三的企業電腦已經受到了某種間諜軟體的感染。

每天都有數千種新型惡意程式變種被釋放出來，而IT工作人員則努力與各種新型攻擊保持同步...IDC認為，幾乎有四分之三的企業電腦已經受到了某種間諜軟體的感染。

此外，垃圾郵件仍然讓企業感到困擾。它以作為其他威脅的一種傳播媒介而被廣泛使用，其中包括了危險的附件或與含有惡意下載、網路釣魚或其他威脅的網站連結。

2008年IDC安全調查表明，對了應對日益複雜的網路攻擊，相應安全防護的架構的變的愈加複雜，這將會是IT專業人員所面臨的最大挑戰。

攻擊者不斷開發創新技術，攻克現有的安全防禦體系，以入侵企業網路。IDC預計，在不遠的未來，"混合式威脅"將更加突出，這必將增加對集成內容安全的需求。攻擊者把各種威脅特徵結合起來，使惡意程式運算法則的變種數量呈指數級增長，以借此找到突破傳統內容安全解決方案的方法。為了實現最佳效果，IT專業人員必須做好準備，針對零時差攻擊、病毒、特洛伊、蠕蟲、間諜軟體、僵屍網路攻擊、Rootkit、廣告軟體、垃圾郵件、網路釣魚、社會工程和很多其他內容安全攻擊的不同組合為公司架構提供保護。正如我們所說，知識就是力量，企業需要廠商提供一種瞭解所有這些內容安全威脅並實施防護的解決方案。

IDC預計，在不遠的未來，"混合式威脅"將更加突出，這必將增加對集成內容安全的需求。

### *攻擊面的擴展*

資訊技術的進步對企業具有極其重大的意義，但是企業卻越來越難在新的複雜變化出現前做好應對方案。依靠網路支援業務活動和應用導致由內部、外部以及企業內的潛在威脅所爆發的攻擊量大幅增長。

越來越多的暴露攻擊面通過互聯網而創建. . . 使得企業在建立"防彈"保護方面面臨巨大的複雜性和難度。

犯罪人員因為希望尋找一種簡單的賺錢方法而發起攻擊，但分佈於各地的分支辦公室、配備筆記本電腦的流動工作者、可攜式設備以及電話、即時通信、語音IP（VoIP）、電子郵件、網站、網路應用接入、Web 2.0以及各種形式的雲計算導致企業在建立針對這類攻擊的"防彈"保護方面面臨巨大的複雜性和難度。

作為一種主要業務應用，電子郵件一直是重點懷疑物件，但是現在網路已然成為首要威脅載體。僅僅打開網頁就有可能被下載惡意程式，用戶只要點擊電子郵件中的連結就會成為受害者，例如查看已被破壞的搜索結果或訪問已被攻擊的可信網站。由於這些簡單的感染方式，企業就必須實施防禦體系，對容易受到攻擊的各個位置--電子郵件來源、電子郵件連結、檔和網頁--進行安全部署，確保威脅在到達企業網路之前就予以攔截。

如果企業未能針對這些新興技術有效地制定政策和／或安全保護，那麼他們可能面臨巨大而代價高昂的風險。

IDC預測，Web 2.0和Business 2.0應用及社區將成為惡意程式分佈、身份詐騙、隱私侵犯以及公司資料丟失的主要緣由。如果企業未能針對這些新興技術有效地制定政策和／或安全保護，那麼他們可能面臨巨大而代價高昂的風險。

企業需要能夠在整個網路內部提供即時保護的內容安全解決方案，同時最大程度地減少解決方案的制定、部署和管理工作。

對於全面的內容安全方法，企業需要通信、網路和終端安全，這樣不論威脅進入網路的何種位置，均可對其予以攔截。不論客戶是否聯網，內容安全解決方案都能針對電子郵件和其他通信方式（即時通信[IM]、移動設備、協作環境等）、網站以及用戶端電腦中含有的威脅提供保護。企業需要能夠在整個網路內部提供即時保護的內容安全解決方案，同時最大程度地減少解決方案的制定、部署和管理工作。時間就是金錢，企業需要減少花在安全管理方面的時間，而把這些時間花在支持發展業務方面的核心計畫上。

## 暫時安全

傳統上，安全解決方案依賴簽名掃描來攔截已知威脅進入網路。這些方法在阻止威脅和遏制爆發方面非常成功，但是傳統的威脅情報的交付方式速度較慢，在發現威脅到執行保護措施之間留出了一段至關重要的空白時間，企業網路有可能在這段時間已受到大面積感染。

傳統方法需要花費大量時間去部署病毒碼。同時要將監測到的威脅進行分析，才能創建保護簽名。一旦獲得特定簽名，該簽名就會被添加到病毒碼中對企業的內容安全產品進行升級。繼而執行以下流程：

- 把病毒碼下載到所有用戶端和伺服器上。這個過程可能需要幾個小時或更多的時間，企業網路無法立即部署保護措施，網路威脅就可以利用這個漏洞時間發起攻擊。
- 定期下載威脅簽名更新。
- 有些解決方案要求掃描網路上的所有內容來識別威脅，其中包括電子郵件和網路流量，從而加大了網路資源的負擔。

除了企業面臨的這些感染性病毒爆發之外，數量激增本身也是一種威脅。由於這些威脅數量的增加，簽名數量也隨之大大增加，使得病毒碼變得更龐大，難以靈活處理，

佔用了太多網路資源並進一步減慢了提供保護的速度。

威脅情報的傳統交付方式速度較慢，從而在威脅發現和威脅保護之間留出了一段至關重要的空白時間，企業網路有可能在這段時間已受到大面積感染. . . 特徵代碼檔難以靈活處理，佔用了太多網路資源並進一步減慢了提供保護的速度。

此外，威脅的數量增加如此之高，以至於對網路都能造成影響。掃描網路中的威脅而不是在源頭處對其進行預期攔截的產品佔用了太多寶貴的網路資源，例如帶寬和存儲等。

### *問題惡化*

很多情況下，企業採用的解決方案方法卻惡化了存在的問題。許多企業分層部署不同廠商的產品，希望這些產品共同針對當今的威脅提供足夠迅速和廣泛的保護。實際上，這種方法不一定會改善有效性，而且此類解決方案也具有增加誤報率的負面影響。

此外，端點產品和功能單一的安全解決方案的分佈已經到了對企業安全變得有害的地步。IT管理員很快就會不堪重負，不僅僅因為所面臨的威脅數量，而且還包括管理和集成採用不同技術、平台和廠商的網路所造成的巨大負擔。與無數控制臺的不斷交互成為了管理員的“巴貝爾塔”。

端點產品和功能單一的安全解決方案的分佈已經到了對企業安全變得有害的地步...與無數控制台的不斷交互成為了管理員的“巴貝爾塔”。

## 讓工作更智慧

### 即時保護

那些在經濟利益驅使下而展開的攻擊所導致的日益複雜的威脅和目標，意味著任何破壞，不論多麼微不足道或多麼短暫，都有可能讓受害企業蒙受巨大損失。IT管理員不斷尋找可以快速而簡單部署的解決方案，最重要的是能夠儘快識別新型威脅並做出迅速反應。從這個意義上，再次證明“時間就是金錢”所言不虛。這種情況下，快速對威脅做出回應的能力能夠為企業節省大量補救費用。而且，“知識就是力量”，新一代安全解決方案必須允許企業從使用垂直獨立式產品向解決方案過渡，在企業應用範圍內共用威脅知識，以提供即時而全面的保護。

把在雲端截毒技術與現場解決方案結合起來可以大大減輕網路負擔，IDC將這種方法稱為混合式安全模式，它可以在攻擊到達企業網路之前更加迅速地做出安全回應，並且顯著減少IT工作人員維護、更新和應對安全類問題所需要的時間。

把在雲端截毒技術與現場解決方案結合起來可以大大減輕網路負擔，IDC將這種方法稱為混合式安全模式，它可以在攻擊到達企業網路之前更加迅速地做出安全回應。

### 信譽服務

基於雲計算的信譽服務是一種智慧的具有適應性的高效安全解決方案，並且因其卓越效用而迅速地普及。這種方法採用了有豐富經驗的的知識資料庫對“聲名狼藉”的電子郵件發送者、網站或檔進行分類，從而攔截並拒絕不良流量和檔案。信譽評等服務能夠以智慧的方法“在源頭處”封堵威脅，發現試圖攻擊處於監控之下的企業系統的混合式威脅。這種方法可以在威脅到達網路之前對其予以攔截，因此節省了寶貴的資源。

基於雲端截毒的信譽評等服務是一種智慧的且具有適應性的高效安全解決方案，並且因其卓越效用而迅速地日漸普及。

現場解決方案部署在雲中時，可使用現場用戶端快速查詢威脅情報，從而減少必須下載到用戶端和伺服器之上的信息量。這種方法減少了網路的負擔，允許企業在安全廠商更新資料庫之後立即獲得最新保護，不再需要等待下載特徵碼和簽名。高級信譽評等服務可以對網路、電子郵件以及終端檔案威脅進行分析，從而發現惡意攻擊。

## 即時保護

管理企業架構是一件非常複雜的事情，尤其是那些大型企業，整個網路有可能處於不斷的升級、拓展和重組之中。企業架構的單個元件可能跨越了多代技術。很多情況下，企業安全解決方案將由多個廠商的終端產品組成。

憑藉混合式在雲端截毒技術，安全應用實現了緊密集成，可以更好地共用威脅情報，從而通過單一管理埠讓IT管理安全政策，監測並報告事件和威脅狀態。這類解決方案只需少數IT工作人員集中控管即可。所有這些優勢都能夠節省時間，節約財力，同時提高安全性。

在雲端的網路安全的混合式防禦方法可以改善企業流程，提高IT專業人員的工作效率。正確配置的安全架構應在企業內部保持透明運行，以便改善日常績效，提高用戶的生產效率，減少安全所需要的IT資源。

# 趨勢科技企業安全

## 創新方法

趨勢科技Smart Protection Network主動式雲端截毒技術，以下簡稱SPN在其高效而集成的雲端截毒技術用戶端架構中提供了一種混合式在雲端方法，雲端截毒技術用戶端架構將為趨勢科技的產品和服務打下堅實基礎。這種創新方法不僅提供即時保護，也大大簡化了設置、管理、監測和維護安全網路架構的複雜性。

趨勢科技是全球最大的安全廠商，自20年前成立伊始一直致力於保護內容安全。趨勢科技始終強調把簡單性和具有全面的安全功能的執行速度結合起來。憑藉其悠久的創新傳統，趨勢科技希望成為雲端安全產品的領導者。趨勢科技企業安全產品由趨勢科技Smart Protection Network主動式雲端截毒技術提供支援，可以為客戶帶來即時保護並降低複雜性，從而減少業務風險和成本。

趨勢科技充分瞭解新興安全格局，同時圍繞趨勢科技Smart Protection Network主動式雲端截毒技術制定了自己的解決方案戰略，趨勢科技Smart Protection Network主動式雲端截毒技術是一種創新的雲安全用戶端架構，將把在雲中技術與羽量級用戶端架構合二為一。

## 趨勢科技Smart Protection Network主動式雲端截毒技術

趨勢科技充分瞭解新興安全格局，同時圍繞趨勢科技Smart Protection Network主動式雲端截毒技術制定了自己的解決方案戰略，趨勢科技Smart Protection Network主動式雲端截毒技術是一種創新的雲安全用戶端架構，將把在雲中技術與羽量級用戶端架構合二為一。雲安全2.0(SPN)囊括了網路、電子郵件的信譽資料庫並且不斷更新相互加強，以提供在雲中威脅情報，實現了即時最新保護，同時消除了與傳統內建式安全解決方案的特徵碼檔部署要求有關的延遲現象和IT費用。

借助雲安全2.0(SPN)，趨勢科技的全球研究、服務和支援中心TrendLabs有超過1,000名專業內容安全專家對威脅資訊進行分析。趨勢科技從眾多來源收集威脅資訊，包括其遍佈全球各地的客戶群體。內置反饋回路為趨勢科技產品和趨勢科技的威脅研究中心及技術之間提供了不間斷通信，從而得以創建完整的威脅情報。

雲安全2.0(SPN)把網路、電子郵件和檔信譽資料庫中的威脅情報互相聯繫起來。如果其中有一種因素顯示不良信譽，則將自動開始攔截受到所有威脅提交方式。行為分析也被用來判斷信譽。單一攻擊的一種元件--例如單一電子郵件或檔--可能看似無害，但是趨勢科技Smart Protection Network主動式雲端截毒技術使用行為分析來縱觀其背後隱藏的關聯，可以判斷在實際上是否存在威脅。憑藉這種先進的互聯掃描能力，潛在有害的電子郵件、網頁或檔就會在到達企業網路週邊之前被予以清除。使用信譽資料庫在源頭處攔截威脅實現了即時保護，降低了複雜性，減輕了網路資源的負擔。

趨勢科技不僅僅只是簡單地提供終端產品類安全方案，而且還在整個網路內部署了保護傳統和新興技術的集成內容安全解決方案，幫助企業避免不斷為安全產品打補丁的工作負擔，借此為網路、訊息和終端構築統一的防禦體系，不論內容安全威脅在何處發起威脅，均可以對其予以攔截。

借助雲安全2.0(Smart Protection Network)，TrendLabs的超過1,000名專業內容安全專家將對威脅資訊進行分析...內置反饋回路為趨勢科技產品和趨勢科技的威脅研究中心之間提供了不間斷通信。

通過趨勢科技智慧保護網路，趨勢科技幫助客戶部署一種全新的安全方法，旨在應對數量不斷增加、複雜性日益加劇的內容安全威脅。雲安全2.0(Smart Protection Network)是一種面向當今威脅環境的更加智慧的安全解決方案。

## 趨勢科技的效用

### *知識就是力量：高效安全，立竿見影*

常言道：事實勝於雄辯。那些依賴電子郵件和網路進行業務活動的趨勢科技客戶以前為垃圾郵件和各種形式的惡意程式爆發而焦頭爛額，現在他們已經看到了立竿見影的效果，從趨勢科技Smart Protection Network主動式雲端截毒技術支持的解決方案中獲益。趨勢科技的一個客戶認為“分分秒秒都在與垃圾郵件發送者作戰”，趨勢科技雲計算技術能夠如此迅速地發揮作用以應對任何網路威脅提供及時保護讓他讚歎不已。

另一位元趨勢科技的客戶表示，電子郵件和即時通信是其業務的重要組成部分。其資訊發送要求24x7x365運行，以生成大量網路訂單。如果這種功能受到破壞，導致數小時無法通信，則將對公司業務造成破壞性的影響。憑藉趨勢科技Smart Protection Network主動式雲端截毒技術所支援的電子郵件和IM安全產品，該客戶實現了"一次設置，終身無憂"的維護狀態，而且客戶堅信因為大量的威脅能夠立即予以攔截，那麼企業必將受到良好的保護。

憑藉趨勢科技，該客戶實現了"一次設置，終身無憂"的維護狀態，而且堅信因為大量威脅能夠立即被予以攔截，那麼企業必將受到良好的保護。

## *時間就是金錢：降低複雜性的內容安全方案*

IT企業始終都在評估各種能夠減少員工系統管理和維護時間的選擇。如前所述，時間就是金錢，但是花在細小而非必要活動上的時間也意味著機會的代價和損失。一名使用趨勢科技託管訊息安全解決方案的IT經理說："我們只需要四名兼職人員來支援我們的訊息通信系統，趨勢科技Smart Protection Network主動式雲端截毒技術帶給我們的最大收益在於取代了我們的人工打補丁和升級工作。現在我們更加主動，因為該方案使我們不再需要花時間去手把手的去處理產品的問題。"

在另一次討論中，一名使用趨勢科技網路安全產品的IT經理表示，在實施趨勢科技的解決方案之前遇到大量間諜軟體和惡意程式問題：「我們在病毒維護方面花費了太多時間。自從使用趨勢科技的解決方案之後，我們就沒有發生過病毒爆發事件。以前我們經常因為宕機而加班加點處理安全問題。現在情況變得好多了，我們再也不需要額外加班了。」

"我們在病毒維護方面花費了太多時間。自用使用趨勢科技解決方案之後，我們就沒有發生過病毒爆發事件。"

趨勢科技的客戶一致希望通過強大的管理平台來節省時間和財力。趨勢科技Control Manager（參見趨勢科技產品描述部分）允許管理員制定全球化政策並將其推向全世界。控制面板為管理員提供中央視圖，以"全面瞭解網路中發生的事情"。趨勢科技Control Manager也是一種提供管理的工具，其中含有顯示趨勢科技產品如何在安全性和用戶生產效率方面提供投資回報的資訊。

## *密切關係創造巨大效益*

通過與趨勢科技客戶進行討論，我們充分瞭解什麼是真正關心客戶成功的公司。一名客戶說："我們和趨勢科技的關係好於以前與任何其他廠商的關係。趨勢科技跟蹤客戶進展和使用狀況；他們能夠不斷獲得回饋資訊，瞭解產品的工作情況以及存在哪些差距需要該進。"

"我們和趨勢科技的關係好於以前與任何其他廠商的關係。趨勢科技跟蹤客戶進展和使用狀況。"

一名在美國和歐洲設有分支公司的國際客戶指出："趨勢科技為全世界的客戶提供支援。該公司提供了出色的支援服務。"

另一名客戶闡述了趨勢科技如何讓客戶取得成功：“趨勢科技的銷售和工程團隊為我們提供了巨大的幫助，這真的讓人無法忘記。我們已經習慣了供應商把軟體交付後就只會祝服我們在以後的使用中能有好運氣這種售後服務模式--然而趨勢科技卻非常積極地幫助我們取得成功，他們為我們提供所需的一切資訊，保證網路部署平穩進行，滿足我們的所有要求。”

“趨勢科技非常積極地幫助我們取得成功，他們為我們提供所需的一切資訊，保證網路部署平穩進行，滿足我們的所有要求。”

## 趨勢科技產品描述

### *趨勢科技的企業產品*

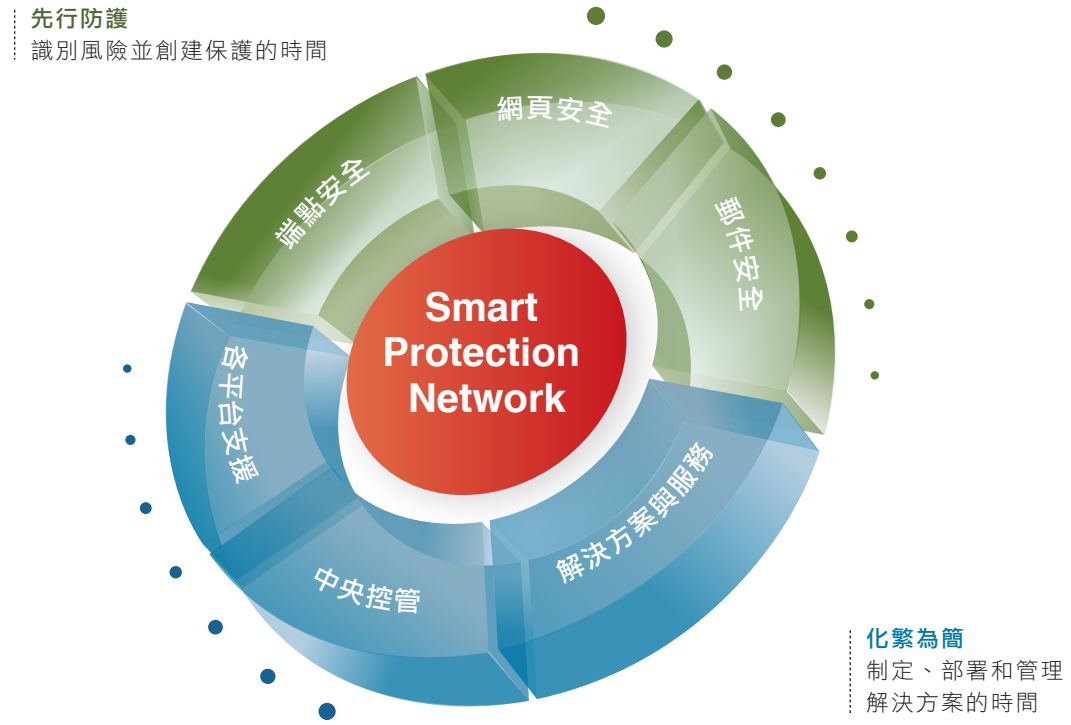
趨勢科技擁有強大的內容安全和威脅管理解決方案產品線。公司不僅提供各種集成解決方案，同時也提供各種可單獨購買的終端產品。不論選擇趨勢科技的某種產品還是完整的安全解決方案，企業都能因Smart Protection Network主動式雲端截毒技術中的互聯威脅情報而獲得更好的保護。

趨勢科技Smart Protection Network主動式雲端截毒技術提供了一種混合式在雲中方法...為趨勢科技的產品和服務打下堅實基礎。

### *趨勢科技的產品和解決方案*

如圖1所示，趨勢科技包括三類主要內容安全產品：網路安全、訊息安全和端點安全。

圖 1




※資料來源：趨勢科技，2008年。

趨勢科技網路安全產品在網路威脅到達網路之前對其予以攔截，使得惡意程式攻擊、網路釣魚、不適當內容以及其他威脅遠離網路，同時憑藉Smart Protection Network主動式雲端截毒技術提供的集成、即時威脅管理方法降低總體成本。趨勢科技還提供網路應用安全來幫助保護企業的網站。這種解決方案可定期或按需執行漏洞評估掃描，自動生成各種專家報告。

趨勢科技訊息安全產品保護企業免受垃圾郵件、惡意程式、網路釣魚、混合式網路威脅、零時差攻擊以及資料丟失等訊息威脅的影響。通過趨勢科技Smart Protection Network主動式雲端截毒技術為訊息安全提供即時保護，同時憑藉託管服務、軟體、虛擬設備解決方案、郵件安全以及IM保護和協作環境降低週邊電子郵件安全的複雜性。此外還提供了基於郵件加密技術和防資料洩露方案的附加安全保護。

趨勢科技終端安全產品採用了行業內獨一無二的先進探測和清除技術的組合，通過利用Smart Protection Network主動式雲端截毒技術的即時威脅情報來保護筆記本電腦、臺式機以及伺服器免受當今複雜的惡意程式威脅的攻擊。不論用戶端是否聯網，在雲中網路信譽都能攔截進出惡意網站的路徑對用戶端施加保護。

全面的套件提供了一種包容性更強的方法，以攔截內容安全威脅。趨勢科技部分套件旨在提供桌面到閘道保護，而其他產品則針對特殊平臺或業務難點提供解決方案。

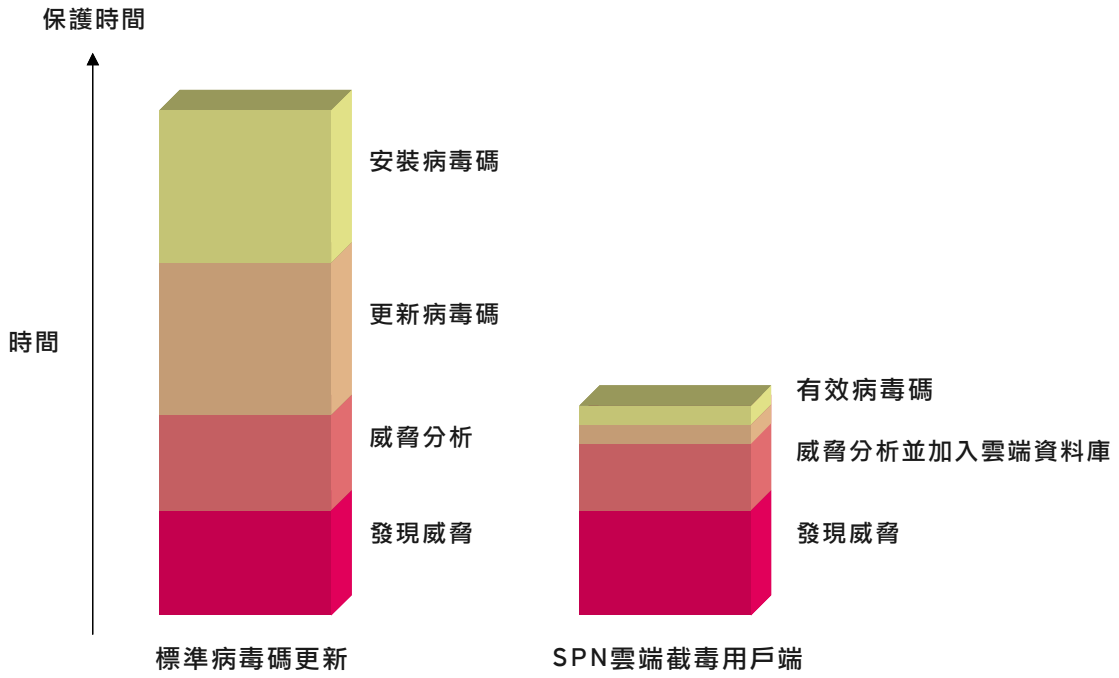
趨勢科技控制管理器提供具備網路控制臺的集中安全管理。控制管理器能更好地瞭解各個用戶端，而無需新增基於用戶端的軟體。控制管理器還能提供綜合更新、全球防禦警報和定制威脅報告。此外，控制管理器還能與趨勢科技爆發預防服務（OPS）共同工作，下載並部署主動的針對具體威脅的政策。

## 領先於網路威脅的挑戰

維護遺留安全系統的IT員工因為要保持相對當今無數日益複雜的網路威脅的領先優勢而承擔了不必要的負擔。這些解決方案不能處理日益增加的威脅數量，佔用了網路資源，因為保護延遲而使得企業暴露于安全鴻溝當中（參見圖2）。

圖 2




※資料來源：趨勢科技，2008年。

此外，若企業採用單獨的終端管理和維護方案進行系統防禦，不僅會加重員工的負擔，而且還必須面臨系統被無法捕捉到的病毒所破壞的風險。成功入侵而造成的宕機或機密資訊被盜所引發的損失是今下任何企業都無法承擔的。IT人員為了避免這種情況發生而必須擔起監督的重任。

傳統的內容安全依賴病毒碼更新，屬於被動防禦方案，而且需要花幾個小時甚至幾天的時間來部署。但是在迅速變化的威脅環境中，攻擊可能來自很多方面並以驚人的速度傳播，這時候傳統方法就會凸顯出其局限性。趨勢科技的雲安全用戶端架構將威脅情報將存放至網路外部的雲中，從而極大的提高了防禦速度。借此趨勢科技能夠更加迅速地更新信譽資料庫，而企業則可以在需要時快速獲得這類資訊--無需等待靜態特徵碼檔的定期更新。

## 結論

內容安全環境變得日益難以管理和防範。垃圾郵件、資料竊取惡意程式、病毒、私密資訊的內部違規、可攜式設備等所帶來的衝擊不斷加大，其速度遠遠快於網路保護者採取防禦措施的步伐。

在討伐攻擊者和垃圾郵件發送者的過程當中，企業可以通過瞭解威脅應對知識來獲得優勢。這種情況下，知識就是了解威脅並提供能夠予以攔截的防禦措施的必要基礎，尤其是對那些最新的漏洞利用工具。傳統解決方案從威脅發現到公佈病毒特徵碼檔需要一段時間，這就會產生不可比避免的延遲現象。在雲中清除威脅可實現最快速的攔截，因為在威脅有機會入侵公司防禦體系之前，保護措施早已啟動並且隨時待命。趨勢科技還將其對內容安全威脅的瞭解以及防禦措施應用到其Smart Protection Network主動式雲端截毒技術架構之中。

趨勢科技緊密集成網路、訊息和終端產品以及服務的解決方案簡化了管理，使得企業減少了花在制定、部署和管理內容安全方案上的時間。憑藉增強的內容安全方案，企業可以將更多精力集中在那些能提高生產效率和創造更多營收的優先計畫上。

## 版權聲明