KASPERSKY

真正的網路安全

Kaspersky Security Solutions for Enterprise

2017

保護企業安全

網路威脅變得較以往更為複雜。若是缺乏能夠有效緩解網路威脅的解決方案，企業就只能任由網路攻擊消耗財務資源、中斷業務連續性、讓機密資料曝光，並且導致信譽受損。無論是哪一種行業，成功的攻擊都會讓任何企業造成極大的損失。

認真看待企業安全

必須為安全入侵付出高昂代價：在卡巴斯基實驗室的 2015 年全球 IT 安全風險調查中，我們發現企業的平均直接復原成本為 551,000 美元，而平均間接成本為 69,000 美元。若要避免這些成本及其相關影響，企業必須強化其 IT 基礎結構的防護類型與等級。

透過利用我們所有產品與服務的基礎，也就是安全情報，卡巴斯基實驗室的解決方案可提供跨各種企業基礎結構領域和新興技術的預測、預防、偵測及回應功能：端點、線上與行動、虛擬基礎結構、資料中心、工業控制系統等。

卡巴斯基實驗室是協助企業升級其安全策略的先驅，目的是以更精良的方式防禦最新進階威脅與針對性攻擊。我們提供的獨家技術和服務組合，是以全球頂尖的安全情報為基礎，可協助企業在針對性攻擊造成嚴重傷害前的更早階段進行偵測並緩解風險。

卡巴斯基實驗室解決方案可透過解決每個階段的 IT 事件，為企業安全提供整體、適性化及策略的方法。我們的理念很簡單：最佳情報結合最佳技術，提供最佳的防護。

端點安全

新一代多層次防護，可防止鎖定您端點的最新複雜與進階威脅

威脅環境的進展速度十分驚人，導致關鍵業務流程、機密資料和金融資源遭遇零日攻擊的風險持續增加。為緩解貴企業組織的風險，您必須比鎖定您的網路專業人員更聰明、設備更精良，而且消息更靈通。不過只有一點是無庸置疑—企業網路攻擊主要是透過端點發動。如果您可以有效保護所有的企業端點、靜態裝置與行動裝置，表示貴組織的整體安全策略有堅實的基礎。

隨著數位商務成長，企業的 IT 環境變得比以往更加複雜。同時，網路犯罪者採用日益複雜的攻擊方法，創造出入侵企業基礎結構的全新方式。

大多數的企業網路攻擊都是透過端點發動。傳統的安全技術缺乏有效的全球威脅情報與機器學習，無法防止高度複雜的威脅。

我們透過進階偵測技術，利用機器學習與威脅情報的組合，可針對未知和進階威脅及針對性攻擊提供零秒防護。

整合加密、自動修補和行動端點防護等強大的控制及資料防護工具，可以進一步強化對進階威脅的防護—全都可以透過 Kaspersky Security Center 進行管理。

所有元件都是由內部開發，並且形成可以輕鬆上手的通用平台，可滿足企業組織持續改變的各種需求。

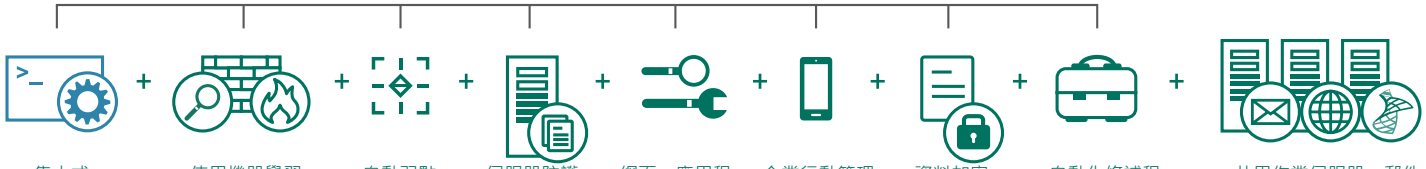
解決方案：KASPERSKY ENDPOINT SECURITY

完整保護所有端點、防止所有形式的進階威脅非常重要。傳統的防毒保護力有未逮，無法提供足夠的防護。唯有採用具備機器學習以進行動態與靜態偵測的先進安全平台，同時利用多層次的防護方法，才有機會為防護層內外的每一個端點提供充分的防護。

我們的技術是以無可比擬的即時威脅情報來源為基礎，即使是最新最複雜的威脅 (包含零日入侵程式)，亦可持續發展為貴企業提供保護。您可選用目前與未來同級產品中最佳的端點防護，將您的安全策略提升至進階威脅探索全球領導廠商的等級。

貴企業組織的安全防護得以邁向新紀元。

Kaspersky Endpoint Security



前所未有的可靠防護，適合所有形式的端點
我們先進的防護技術可以保護企業組織及其 IT 基礎結構，從實體和虛擬桌面與伺服器到行動裝置的所有端點，無論結構有多複雜都可獲得保障。

利用機器學習的行為分析可保護貴企業
我們的解決方案使用以靜態和動態資料技術為基礎的機器學習。這是我們保護您的方式，即使是未來的威脅也可加以防護。

強大的全球威脅情報
我們所有的技術都是由我們經過驗證的全球威脅情報提供技術支援。我們在 APT 方面的研究比其他安全供應商都還要多，因此對現代威脅本質的了解程度無人能及，可協助您更妥善防護這類威脅。

自動化的即時回應
當我們的動態行為監控引擎偵測到威脅時，系統會自動回溯惡意程式造成的任何變更。

可防止零日威脅與入侵程式的連續動態防護
自動弱點入侵防護的開發目的，在於防止網路犯罪者鎖定受保護電腦中的應用程式弱點。自動化修補程式管理為安全防護新增額外的防護層。

通過 FIPS 140-2 認證的資料防護
使用者無法察覺的強大加密，可在您外出時充分保護機密和敏感性資料，不管資料是位於可攜式裝置還是原本的裝置內。

可靠的勒索軟體防護
我們的防勒索軟體技術可持續保護您的資料安全、防止網路犯罪者獲得贖金資助、防護共用資料夾遭到進階的加密鎖定軟體攻擊。

透過整合與集中管理，實現更低的總持有成本 (TCO) 和更高的投資報酬率 (ROI)
利用相同的主控台管理多個平台與所有的端點裝置—提升可視性與控制能力，不需額外投資軟體、設備或人力資源。