VMware NSX Advanced Threat Prevention

VMware NSX Advanced Threat Prevention (ATP) 這款解決方案可使用機器學習來識別和防禦進階威脅，進而強化資料中心防火牆。

透過 Advanced Threat Prevention 強化防火牆

在機器學習的支援下，VMware 適用於 NSX Service-defined Firewall 的 Advanced Threat Prevention (ATP) 方案可提供網路流量分析、入侵偵測與防禦，以及具備全面性網路偵測與回應功能的進階惡意軟體分析。此解決方案是專為保護資料中心流量所打造，具備業界對進階威脅的最高精確度洞悉見解。

探索 Service-defined Firewall

運用包含具狀態的第 7 層存取控制與進階威脅防禦的新一代內部防火牆，保護您的資料中心。

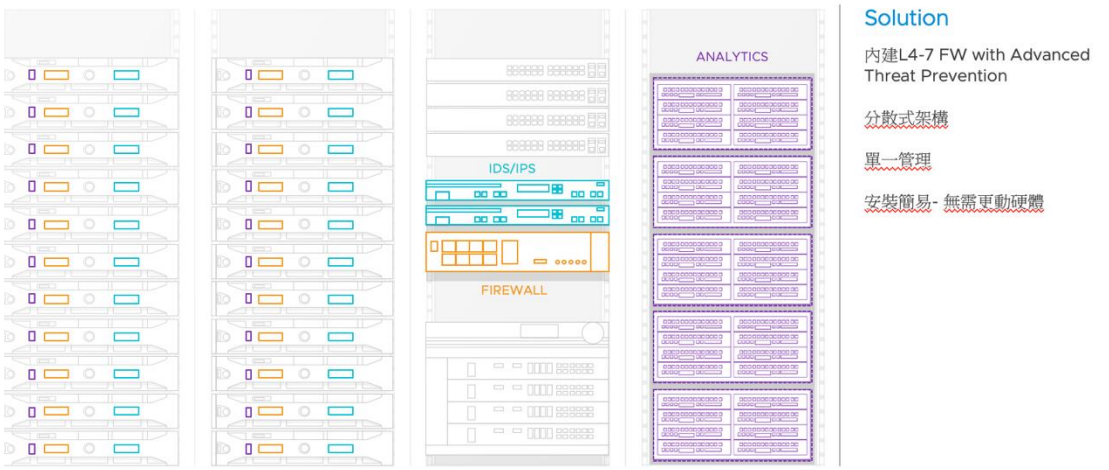
NSX Advanced Threat Prevention 的優勢

取得無所不在的威脅能見度

透過深入的能見度，同時運用多種威脅偵測技術，以檢測所有資料中心的流量是否存在威脅。

NSX採分散式不用怕邊界被突破

零視角方案



防範進階惡意軟體

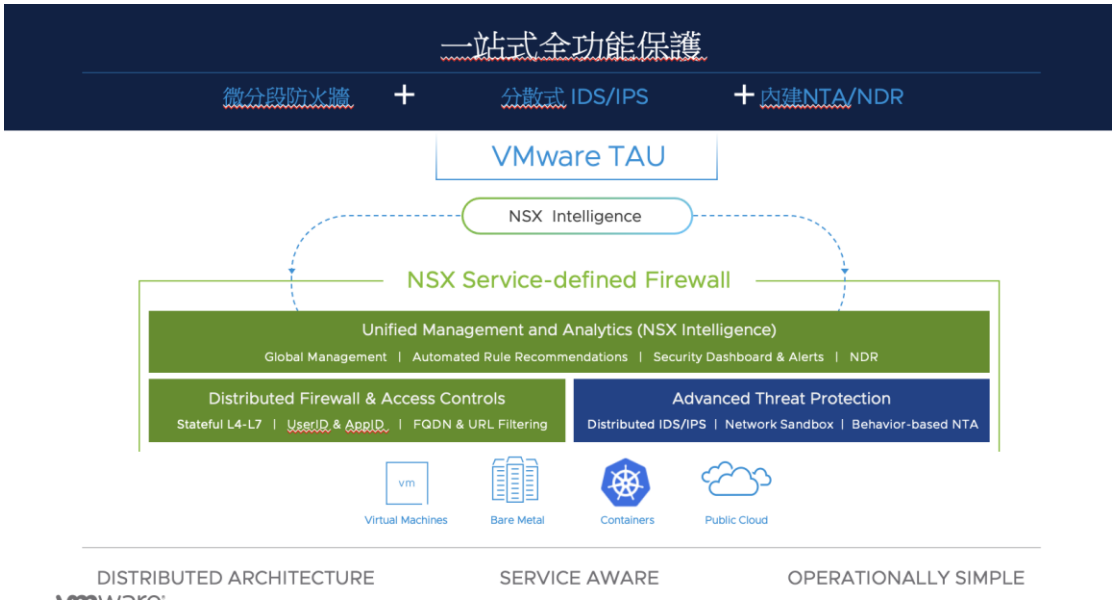
有些惡意軟體是為規避標準安全性工具而設計，運用 Advanced Threat Prevention 即可偵測這些惡意軟體。

著重在真正的威脅

將誤報數量減少達 90%。提高警示的準確性，讓您的安全團隊能專注於小部分的真正入侵。

進化為主動搜尋威脅

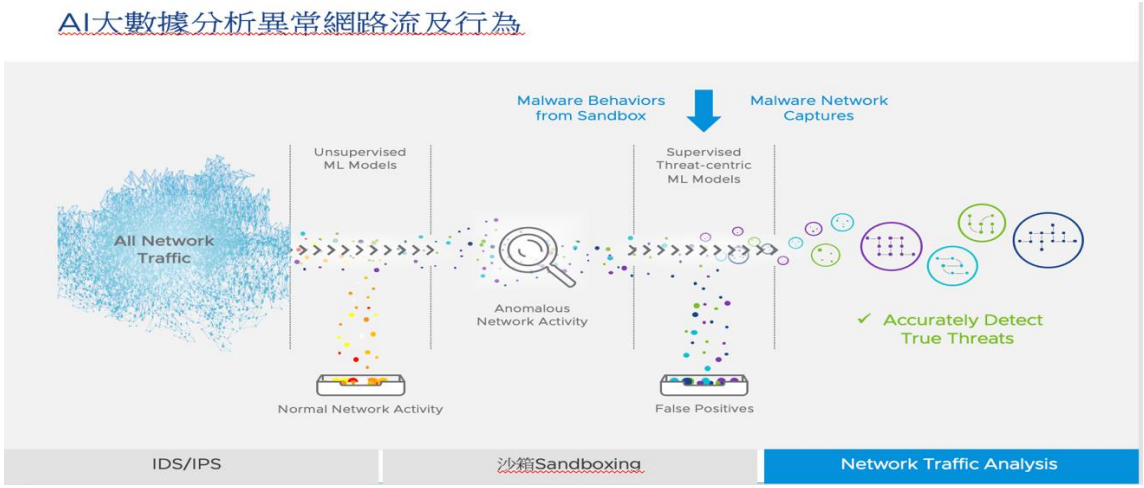
不僅僅是回應警示。在新出現的威脅影響到業務之前主動找出。



VMware NSX Advanced Threat Prevention 的主要功能

偵測威脅

根據精確的應用程式情境來運用精選簽名，以偵測所有東西向流量中的已知威脅。

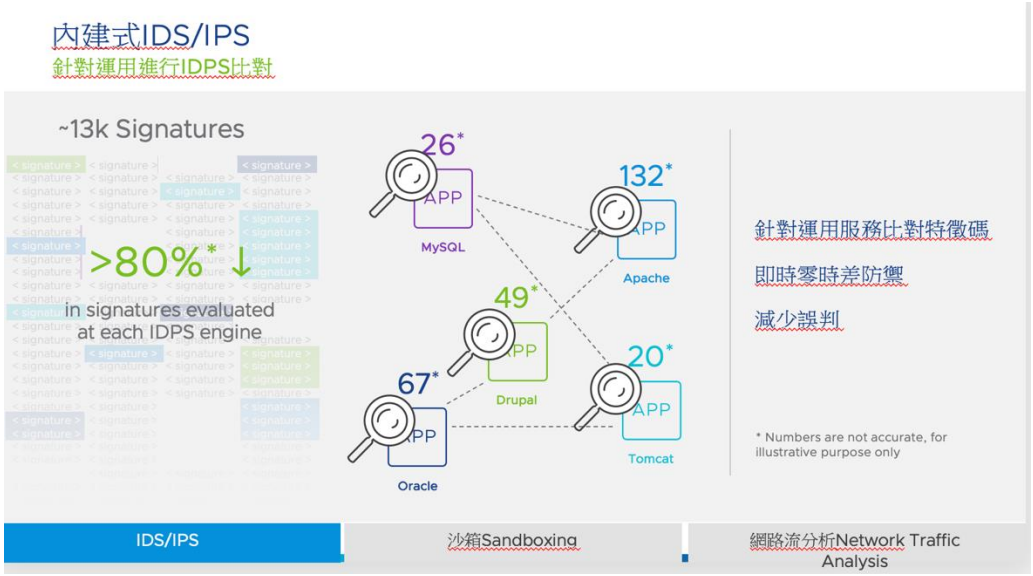


識別異常

使用監督式及非監督式機器學習，在整個網路中找出異常活動與惡意行為。

尋找惡意內容

透過硬體模擬和監督式機器學習模式，尋找經由網路傳輸的惡意內容。



關聯資料

透過關聯性引擎來篩選大量的網路資料和事件，以排除誤報與零入侵，從而防堵小部分的真正入侵。