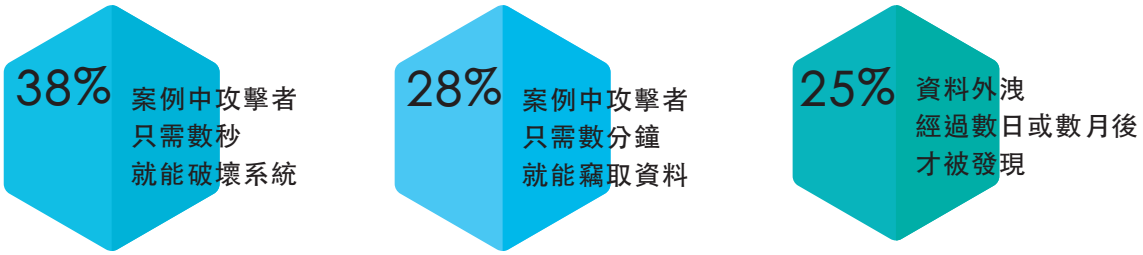
中芯數據
Core Cloud Tech.

內網威脅防禦管理系統

奪回系統真正主控權

2015年起爆發了多起大型資安事件，造成機敏資料外洩，　　包括影片檔、員工與主管個資和薪資等。如SONY 至少砸下數千萬美元來全面清理更換電腦系統，這還未加上機敏資料外洩的損失。當入侵發生時，你該如何面對？你知道你已經被駭了嗎？

面對不可能完全避免的APT問題，企業的防禦機制應著重於如何加速惡意程式的識別及事件處理的回應速度，才能有效降低數位資產被竊取的風險。透過導入中芯數據　“內網威脅防禦管理系統”，徹底奪回您的端點的控制權。利用持續性的分析機制，即時處理資安事件，將重要資料外洩的機會降到最低。



資料來源：2015 Data breach investigations report

管理介面

中芯數據內網威脅防禦系統部署威脅收集器至需防護的端點設備，可即時分析並發送警報通知管理人員。您可以清楚的了解目前受到的APT威脅狀況。並且簡單迅速的排除威脅。內網威脅防禦管理系統提供以下資訊：

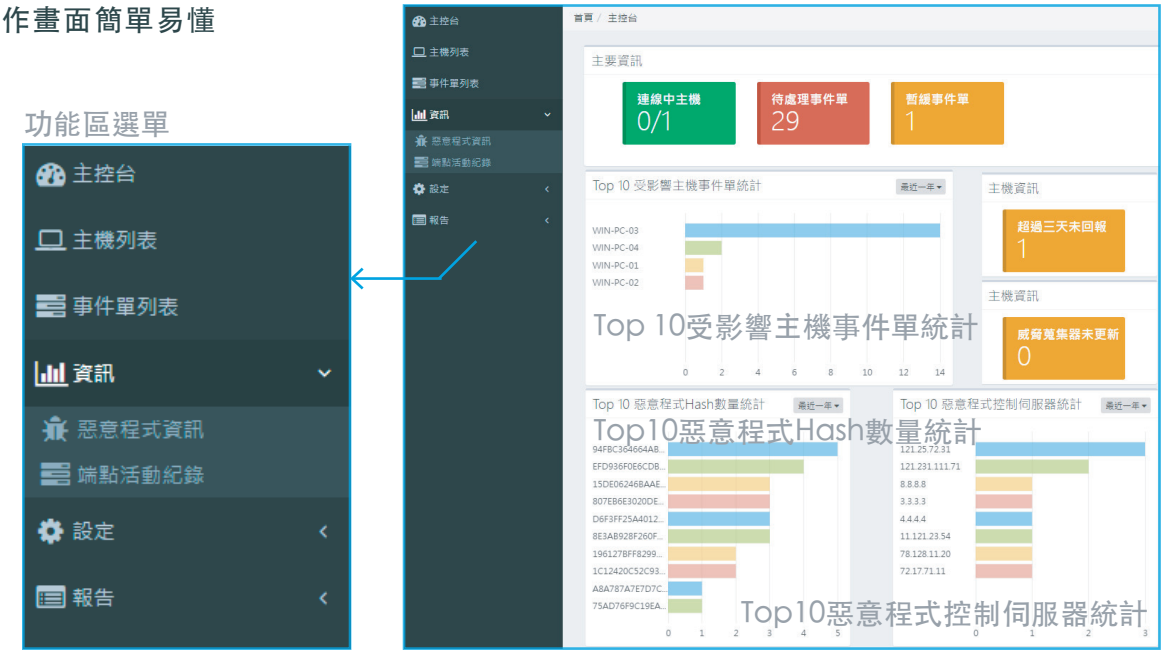
主機資訊 透過內網威脅分析平台提供的主機清單，您可以一目了然的了解目前受到保護的主機狀態，並且檢視各主機受到威脅狀態。

事件資訊 可檢視系統通報單。透過事件單列表，您可以看到目前發生的威脅及已排除的威脅。您可以進一步檢視經過系統分析的威脅資訊，並且快速排除威脅。

定期事件報告 透過惡意程式列表和擴散路徑分析，您可以了解對單位受到的內網威脅狀態，針對擴散路徑進行防堵或人員資安訓練強化。已減低未來再次發生資安事件的風險。

中芯數據股份有限公司
APT事件處理小組
0809.016.818
www.corecloud.com.tw

Dashboard主操作畫面簡單易懂



主機列表：由主機列表中，您可以看到目前受監控主機的狀態。

事件單列表：您可以由事件單列表檢視由專業資安人員分析後確認的資安威脅。

內網威脅防禦管理系統

>內網端點威脅防禦管理系統2021標準版
>內網端點威脅防禦管理系統2021專業版
>內網端點威脅防禦管理系統2021白金版
>內網端點威脅防禦管理系統2021基礎版
>主機威脅防禦管理系統2021版
>網站威脅防禦管理系統2021版