

User's perspective

如何**即時掌握**內、外部的資安威脅警訊?

如何**降低**資安佈署的複雜度、人力及維運成本?

如何**淨化**我的連外網路頻寬? 提昇頻寬使用率及對外服務品質?



客戶

為甚麼攻擊事件還是持續不斷?
如何**輕鬆掌握**防護成效? 誰是**值得信賴**的專家?

Level 1.建置簡易防火牆、限制對外連限、購買防毒軟體

or

Level 2.委由軟硬體供應商建置資安設備，委託或自行管理

or

Level 3.資安服務商 費用高昂(建置專屬專用資安設備及駐點人員)

ISP's perspective

以服務為宗旨，建立安全可靠的網路應用環境，
提供客戶輕鬆佈署且有效的解決方案

藉由設備共享與集中管理，協助客戶簡化資安佈署、
大幅度減少設備成本、維護人力與時間的投入

從ISP機房網路最前端即進行防禦，淨化頻寬，
提高客戶頻寬效益及其連外服務品質

開發HiNet網路資安威脅分析及擴散病毒樣本搜集，
提供即時阻擋服務，避免擴散，有效防護

建立資安事件申訴管道及監看處理服務，
協助國內外網路user資安事件處理及追蹤

- 資安事件申訴處理
- 客戶資安事件協助處理
- 客戶網路釣魚(Phishing)詐騙事件處理
- 客戶濫發垃圾郵件及垃圾網站(URL)處理

