

# 網路記錄器

# IDR-1000C



新軟網路記錄器 IDR-1000C 是一款功能強大的網路側錄、管理工具。可整合企業 AD 伺服器網域環境，詳細記錄旗下員工的上網情況 - 所瀏覽的網頁、Web Mail 所收發的信件、一般電子郵件 (SMTP、POP3、IMAP)、即時通訊 (Skype[語音/文字]、Yahoo 即時通、ICQ、QQ...)、FTP 及 Telnet。

並且提供網路行為管理，以協助企業保護其資料安全，並可用來遏止員工於上班時間利用企業網路資源從事私人活動，有效提升工作效率，是網路安全系統中不可或缺的管理利器。

## 產品功能

### 完整記錄常用網路服務，遏止員工摸魚歪風

IDR-1000C 可以詳細記錄一般使用者最常使用的八大項網路服務，舉凡網頁瀏覽 (HTTP)、收發信件 (E-mail、Web Mail)、即時通訊聊天 (Skype、Yahoo Message、QQ、ICQ)、檔案下載 (FTP)、Telnet (BBS) ... 都可以詳加記錄。管理人員可對企業網路的使用情況一覽無遺，輕鬆了解員工在上班時間都利用企業網路資源在做甚麼，遏止員工網路摸魚歪風盛行。

### Skype 文字 / 雙向語音記錄

IDR-1000C 除了可記錄 Skype 的文字訊息外，亦提供了“雙向”語音記錄；以雙聲道記錄著 Skype 語音對話內容。左聲道為內部使用者的聲音 (記錄擁有者)，右聲道則為遠端對象，兩者聲音完全做分離。倘若日後如有發生特殊狀況需作聲紋比對時，兩者聲音並不會因此互相干擾而誤判。

### 內建網頁郵件分析引擎

市售網路側錄設備大多採用網頁快照方式記錄網頁郵件；這種記錄方式僅將網頁郵件視為一般網頁在做記錄而無法明確區分收件者、寄件者、主旨、郵件內容、附加檔案... 各種郵件要素，導致事後找尋、瀏覽信件異常艱難 (僅能以使用者、時間、網頁郵件網站... 找尋信件)。而 IDR-1000C 所內建的“網頁郵件分析引擎”可自動分析網頁郵件之各項要素，再加以重組、記錄。網頁郵件報表清晰明確，搜尋功能完整容易。

### 簡單易用的控制介面 清晰易懂的多種記錄圖表

具有繁體中文、簡體中文、英文三種語言且簡單易用的操作介面。提供各項系統資訊、各類流量統計並均以智慧化圖形顯示，使管理者易於分析判斷。

### 透過行動裝置 APP，隨時隨地了解網路使用情況

提供企業管理階層專屬的行動裝置 APP (支援 iOS、Android)；就算是出國洽公在外，透過智慧型手機、平板電腦... 行動裝置還是可以輕鬆取得 IDR-1000C 所回饋之各項訊息，快速掌握員工上網情況、即時通訊聊天內容...



### 瀏覽找尋記錄方便簡單、詳細清楚

IDR-1000C 的記錄瀏覽方式特別針對一些不諳網路之管理者 (老闆) 所設計；管理者可輕鬆找尋調閱各項記錄，不會有關讀上的隔閡問題。

- ◆ 介面採用 UTF-8 編碼方式設計，多國語言之記錄可同時呈現；不需頻繁切換瀏覽器即可觀看各種語言記錄，適合跨國交易頻繁的企業使用。
- ◆ 多種記錄閱覽方式 (依網路服務種類、依使用者、使用者今日記錄...) 與全方面搜尋機制，讓管理者可輕鬆找到所要的資料。
- ◆ 直覺式記錄列表設計；記錄列表以使用者名稱、網頁抬頭... 方式呈現，僅看記錄列表就可明瞭各項記錄的涵義，讓不諳網路的管理者 (老闆) 亦可輕鬆上手。

使用者	時間	網頁
王大明	10:32	外資：2年內經濟難
孫小毛	10:35	PChome線上購物
丹丹	10:36	HiNet論壇區
192.168.1.35	10:36	http://tw.news.yahoo.com
192.168.1.21	10:42	http://shopping.pchome.c
192.168.1.54	10:45	http://tw.stock.yahoo.com

直覺式記錄呈現 輕鬆好閱讀！

舊式記錄列表 不知所云！

## 多種記錄資料整合方式，適用於各種網路環境

為了釐清每筆記錄資料的歸屬，IDR-1000C 提供了多種“記錄資料與使用者整合方式”供企業選用。

**整合 AD 帳號** - 可整合企業 AD 網域環境，以人 (AD 登入帳號) 為記錄基準。

**整合認證帳號** - 使用者需通過認證後方能上網，IDR-1000C 將以使用者帳號作為記錄基準。(無 AD 網域環境之企業亦可以透過此模式達到，以人為記錄基準之需求。)

**整合 IP/MAC** - 可依企業網路環境，選擇以 IP 或 MAC 做為記錄基準。

## 異常流量偵測功能

當內部電腦發生中毒之情況，不斷發送封包企圖癱瘓企業網路時，IDR-1000C 會立即發送警訊告知中毒電腦的使用者及管理員，以便即時排除問題之所在。如 IDR-1000C 採用橋接模式架設，則將可再進一步阻擋此攻擊封包傳送，讓其他使用者可正常上網。倘若企業亦有架設「核心交換機」，IDR-1000C 可與其協同防禦企業網路；可封鎖攻擊來源所銜接之交換機網路埠，避免疫情擴散。

## 以階層化方式，分層管理企業網路

企業每日上網資料成千上萬，檢視這些資料並不是一兩個管理員可處理的工作。因此可藉由內建之群組管理員機制，將記錄瀏覽權限分散給各部門主管 (群組管理員)；由部門主管負責該部門的網路資料 (部門主管亦僅能瀏覽該部門之資料，不用擔心機密資料會讓不相干的人員取得)。透過分層管理方式，輕鬆掌握企業網路使用情況。

## 協助企業管理網路應用軟體

一般企業所架設之防火牆並無法有效管控日漸蓬勃發展的網路應用程式，易成為企業網路一大隱憂。為此，IDR-1000C 特別加入了相關管理機制以協助企業掌握其運用。

**即時通訊管制** - 可跟據企業網路政策，妥善管理 ICQ、Yahoo、QQ、Skype... 即時通訊使用情況 (禁止聊天 / 傳檔)；允許使用者記錄其聊天內容，禁止使用者則阻擋之，以達到“有效開放，積極管理”之目的。

**P2P 阻擋機制** - 可封鎖 eMule、BT、Foxy、迅雷... 點對點軟體，以避免企業網路遭到濫用。

除了上述的即時通訊、P2P 軟體，IDR-1000C 亦可管控影音軟體、線上遊戲、穿牆軟體、遠端控制... 多樣的網路應用程式；輕鬆控管網路應用程式使用情況，確保企業網路安全。

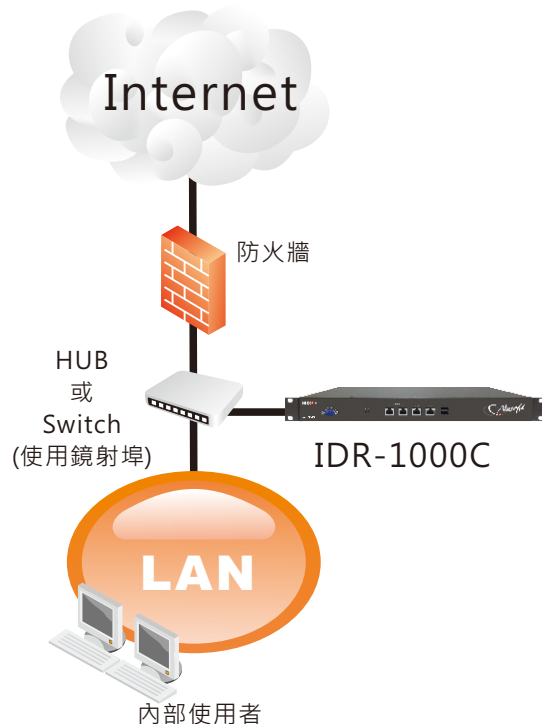
## 透過硬碟空間分配、NAS 遠端備份，輕鬆保存重要資料

一般網路側錄設備的記錄保存方式通常採用“先進先出”這原則運作，導致企業所著重之信件、即時通訊記錄容易被較不重要且龐大的記錄 (網頁瀏覽、FTP...) 所排擠。因此 IDR-1000C 特別著重其內建硬碟的空間分配方式；藉由調整各種記錄的保存期限，以達到妥善分配硬碟使用空間之目的。

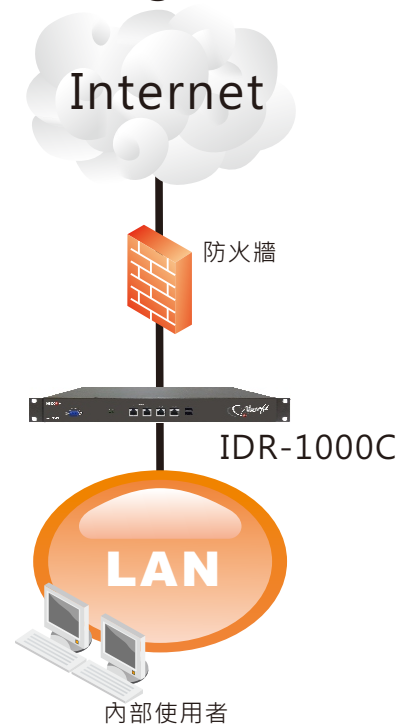
另外，IDR-1000C 亦提供了遠端備份機制，定時將重要記錄資料備份至 NAS 中長期保存。不管在何處 (在家裡、國外出差...)，管理者只需利用瀏覽器 (不用額外安裝任何軟體)，透過 IDR-1000C 的介面就可直接搜尋、瀏覽、取回這些備份資料，相當輕鬆、方便。

## 架設環境

### 1. Sniffer 模式



### 2. Bridge 模式



產品特色

新軟網路記錄器特點	可帶來的好處	它牌網路側錄設備
內建WebMail分析引擎	內建Web Mail分析引擎；可解析“網頁郵件”的各項資訊（收件者、寄件者、主旨、內文、附加檔案...）並重組成“信件”後加以保存。管理者可輕鬆瀏覽、找尋需要的郵件。	將網頁郵件以“網頁快照”方式記錄，系統無法判別信件的各項資訊，管理人員僅能就何人、何時、去哪個Web Mail網站...無關緊要的條件搜尋信件。
閱讀輕鬆的直覺式記錄列表設計	採用UTF-8編碼，並針對不黯網路的老闆所設計；僅看記錄列表就可明瞭各項記錄的含義，適用於跨國業務頻繁的企業。	無法同時呈現各國語言之記錄，且記錄列表閱讀困難。想要完全了解記錄列表之含義，還需要調閱其他相關資料。
「可整合AD網域環境」與「認證上網暨整合記錄功能」	可以使用者之AD帳號作為記錄依據，或以網路記錄器的認證上網機制之“認證帳號”作為分類依據。	僅只有以IP或MAC作為記錄之依據，無法與AD網域環境整合。
行動裝置APP瀏覽記錄	提供行動裝置專屬APP（支援iOS、Android），可隨時隨地掌握企業員工網路使用之情況。	記錄瀏覽界面僅針對一般桌上型、筆記型電腦設計，用手機瀏覽器觀看極為不便。
Skype文字、語音記錄	提供Skype的文字訊息與“雙聲道”語音記錄；將發話者與收話者的區隔為左右聲道，以方便日後聲紋比對之用。	絕大部分不提供Skype記錄功能。即使可記錄Skype，則僅能記錄文字或“單聲道”語音記錄。
提供多種閱覽與搜尋機制	多種記錄閱覽方式（依使用者、服務種類、使用者每日記錄...）與全方面搜尋機制，讓管理者輕鬆找到所要資料。	僅只有依服務種類分類記錄，瀏覽不便。且其搜尋功能陽春，不堪使用。
可調整各種服務記錄保存時間	可依每種記錄之重要性調整其保存期限，進而達到重要資料長期保存之目的。	記錄資料以先進先出方式保存（最早資料優先覆蓋），無法依服務重要性調整。
採用NAS遠端備份	記錄資料可自動備份至遠端NAS，管理者可隨時隨地的瀏覽、搜尋遠端備份記錄。	採用手動光碟燒錄備份方式；備份不方便、保存不易、資料調閱困難...。
群組管理設計	部門主管僅能瀏覽該部門的記錄資料。以階層式管理機制，分層管理企業網路。	次管理員可看到所有記錄資料，連不該看的也都全看到了。
MSExchange內部網路郵件記錄	提供針對MS Exchange的Journaling 郵件記錄功能，可記錄內部網路之溝通信件。	當用MS Exchange為郵件伺服器時，無法記錄內部網路之溝通信件。
網路應用程式管制	內建即時通訊、P2P、穿牆軟體...管制機制，輔助企業管理這些網路應用程式之使用。	無提供此功能，企業網路易被濫用。
異常流量防禦	倘若企業內部發生DoS飽和式攻擊企圖癱瘓企業網路時，新軟網路記錄器可立即截斷攻擊並通知管理人員，以確保企業網路正常運作。	無提供此功能，遇到內部攻擊時束手無策。
每筆即時通訊記錄自動區隔	在記錄即時通訊時，會自動將不同聊天對象之記錄區隔保存，記錄內容簡單明瞭、不易混淆。	所有即時通訊記錄像大雜燴一樣混雜在一起，不易了解聊天內容。



網路記錄器規格比較表

產品型號		IDR-800C	IDR-1000C	IDR-1500C	IDR-2500	IDR-3500
<b>硬體規格</b>						
硬碟		500 GB	500 GB	500 GB	1 TB	1 TB
連接埠數		4 (Giga 埠)	4 (Giga 埠)	4 (Giga 埠)	4 (Giga 埠 / Mini GBIC)	4 (Giga 埠 / Mini GBIC)
HW Bypass功能		×	○	○	○	○
安裝佈署	橋接模式	○	○	○	○	○
	旁接模式	○	○	○	○	○
無風扇超靜音設計		○	×	×	×	×
外觀尺寸		9" 桌上型	1U 機架式	1U 機架式	1U 機架式	2U 機架式
<b>軟體功能</b>						
服務記錄	電子郵件	○	○	○	○	○
	網頁瀏覽	○	○	○	○	○
	即時通訊	○	○	○	○	○
	網頁郵件	○	○	○	○	○
	FTP	○	○	○	○	○
	Telnet (BBS)	○	○	○	○	○
群組管理員		○	○	○	○	○
行動APP記錄瀏覽		○	○	○	○	○
記錄依據	IP / MAC位址	○	○	○	○	○
	AD登入名稱	○	○	○	○	○
	認證名稱	○	○	○	○	○
記錄分類	依網路服務	○	○	○	○	○
	依使用者	○	○	○	○	○
遠端備份	NAS / File Server	○	○	○	○	○
	線上瀏覽	○	○	○	○	○
行為管理	即時流量分析	×	×	○	○	○
	異常流量偵測	○	○	○	○	○
	即時通訊管制	○	○	○	○	○
	應用程式管制	○	○	○	○	○