Highter®
Secure your information
海德資訊科技股份有限公司
+886 2 2659 6326 www.highter-tech.com.tw

Retie Shield
最佳資訊安全防護暨帳號管理系統

協助您建置多種平台多層次的(Multi-level)帳號管理與存取控制安全管理政策

主動式提供**完全防護**避免您的系統被入侵

功能特色：

- 主機式防火牆與弱點程式保護
- 主動式完全防護駭客與惡意程式入侵
- 強制型防護重要程序、服務與檔案
- 強化 Console Mode 安全與活動軌跡查核
- 異質平台統一安全政策管理
- 異常與重要活動即時告警、查核與驗證
- 完整且無法規避的系統活動監控與軌跡記錄
- 圖型化的遠端集中式管理

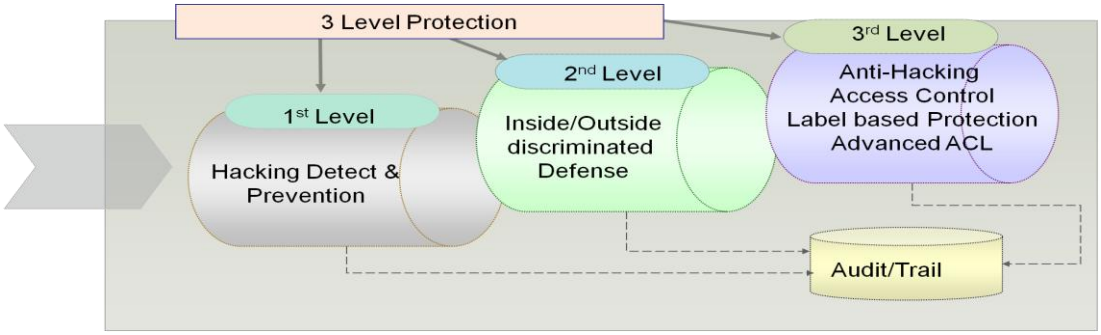
B1 安全等級

三層式安全防護架構，強制型存取控制MAC (Mandatory Access Control)與完整的系統監控，提供B1安全等級的防護，確保資訊安全政策的落實而非使用者個人的自由心證。

- 避免惡意使用者存取：合法使用者不能存取超越其所被允許的系統權限之資源。 所有的存取運作完全基於企業管理政策。
- 主動防止惡意攻擊程式入侵。

可保護： 應用程式、系統資源、資料、執行中程序與使用者帳戶。

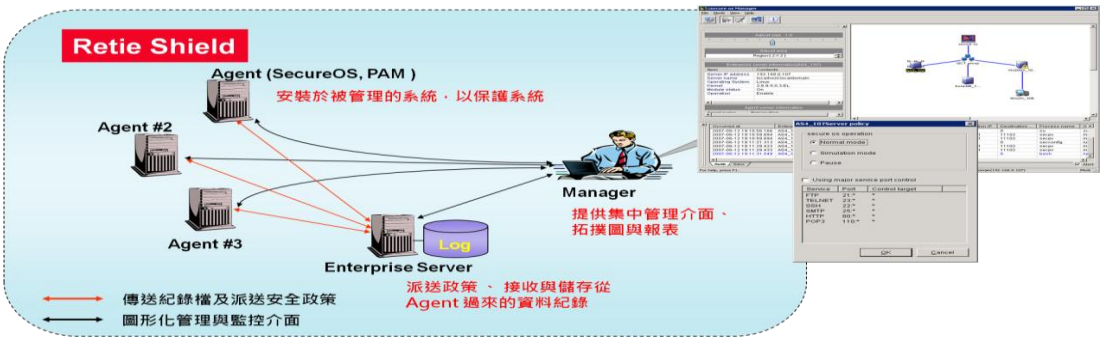
- B1安全等級為美國國防部公佈之評價IT系統的安全和可靠性的標準，一般商用系統等級為C2，安全等級更高的B1一般稱之為"可信賴的作業系統"（Trusted OS）



集中式管理

提供簡便的政策派送與管理方式。

遠端中控平台，以圖形介面提供查詢與設定，並提供系統資源狀態顯示；資訊安全政策可以群組或者單一方式派送至每台主機。



資源隔離

提供系統資源安全標籤隔離政策，強化重要檔案、指令、程序與帳號的安全。

可以掌控每個檔案(File)或每個程序(Process)對於系統及其它元件的存取權限，同時根據實際需求，給予不同的權限，而達到責任區分(Separation of Duties)的目的。

加強型認證

提供系統管理員(System Administrator)與安全管理員(Security Administrator)雙重認證，以區分系統管理及安全政策管理之權責。

- 增強型認證模組PAM (Pluggable Authentication Modules)可對使用者帳戶提供強化且強制的帳戶及密碼管理。

全面資源管理

針對每一個系統使用者帳戶，登錄碼(Registry)、程序(Processes)、檔案(Files)、共享資源(Shares)及服務(Services)…等，全面落實權責管理政策。

- 間諜程式、蠕蟲、病毒與任何的惡意程式，無法自行複製與安裝入系統。
- 登錄碼(Registry)控制模組能夠防止此一類型的所有入侵行為。
- 強化 Console Model 使用安全，並完整記錄其活動軌跡，滿足維運與安全人員之需求。

駭客防護

以權限控管為基礎的防護機制，防止駭客非法入侵存取系統。

- 使用強制型存取控制(MAC)功能，即使伺服器具有系統弱點，亦無法對系統造成傷害 (例如，因系統弱點造成Buffer Overflow漏洞)。
- 惡意程式無法感染系統，因為沒有足夠權限存取系統檔案。

即使駭客成功的進入系統，也無法對運作中的系統造成影響，甚至駭客取得最高管理權限(root/administrator)，還是無法存取其它的檔案或物件，主動式的防禦確保系統安全。

入侵偵測防護

以行為模式為基礎的入侵偵測系統，可有效偵測任何的非法存取企圖，並針對系統重要的檔案、服務、程序與帳號，執行即時查核與驗證的功能。

整合式防火牆

區分來自內部/外部的防禦，提供防火牆的防護，對系統完整的連線控制。

- 強化重要帳號連線登入服務，如監控外包商高授權帳號使用的風險。

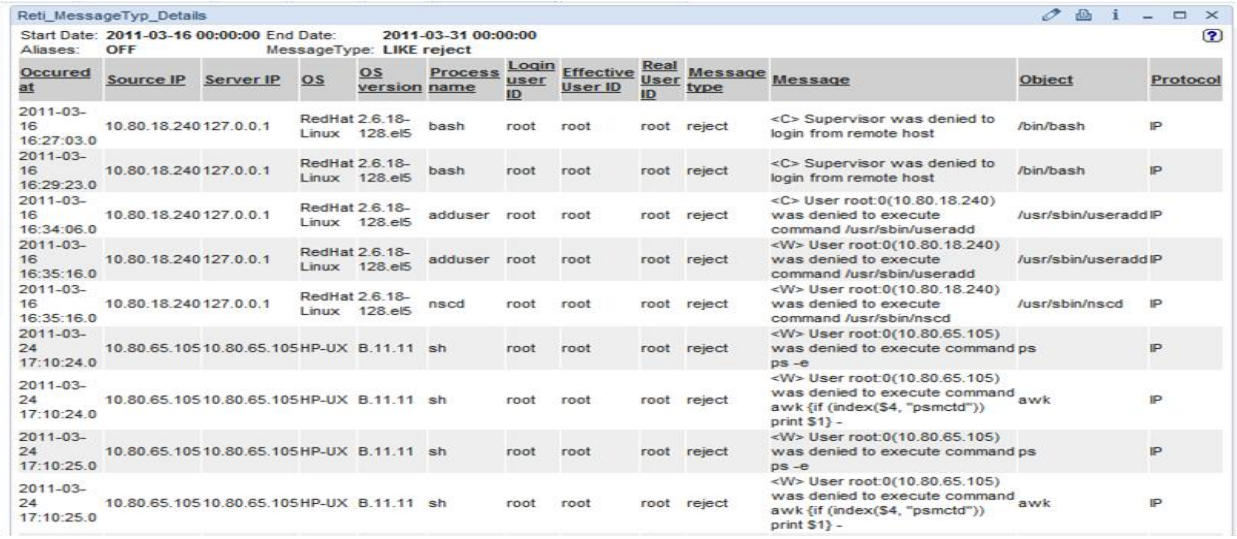
圖型化管理介面

提供系統安全管理拓樸圖，以單一圖形介面管理完成設定與稽核。

- 集中式的安全管理與政策派送，以降低政策佈署及管理負擔。
- 即時報表與詳儘的日誌監控。

稽核需求

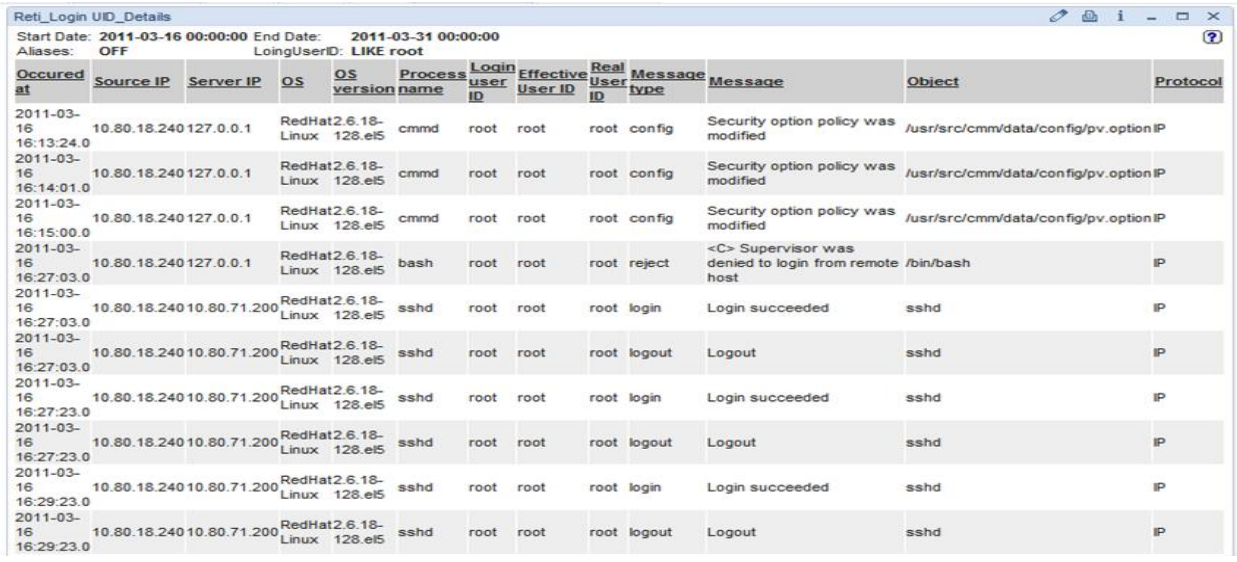
提供即時稽核、日誌及統計報表、且稽核資料被集中儲存及保護、以確保稽核工作可順利進行。



Reti_MessageTyp_Details

Start Date: 2011-03-16 00:00:00 End Date: 2011-03-31 00:00:00
Aliases: OFF MessageType: LIKE reject

Occured at	Source IP	Server IP	OS	OS version	Process name	Login user ID	Effective User ID	Real User ID	Message type	Message	Object	Protocol
2011-03-16 16:27:03.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	bash	root	root	root	reject	<C> Supervisor was denied to login from remote host	/bin/bash	IP
2011-03-16 16:29:23.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	bash	root	root	root	reject	<C> Supervisor was denied to login from remote host	/bin/bash	IP
2011-03-16 16:34:06.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	adduser	root	root	root	reject	<C> User root:0(10.80.18.240) was denied to execute command /usr/sbin/useradd	/usr/sbin/useradd	IP
2011-03-16 16:35:16.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	adduser	root	root	root	reject	<W> User root:0(10.80.18.240) was denied to execute command /usr/sbin/useradd	/usr/sbin/useradd	IP
2011-03-16 16:35:16.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	nscd	root	root	root	reject	<W> User root:0(10.80.18.240) was denied to execute command /usr/sbin/nscd	/usr/sbin/nscd	IP
2011-03-24 17:10:24.0	10.80.65.105	10.80.65.105	HP-UX	B.11.11	sh	root	root	root	reject	<W> User root:0(10.80.65.105) was denied to execute command ps -e	ps	IP
2011-03-24 17:10:24.0	10.80.65.105	10.80.65.105	HP-UX	B.11.11	sh	root	root	root	reject	<W> User root:0(10.80.65.105) was denied to execute command awk {if (index($4, "psmctd")) print $1} -	awk	IP
2011-03-24 17:10:25.0	10.80.65.105	10.80.65.105	HP-UX	B.11.11	sh	root	root	root	reject	<W> User root:0(10.80.65.105) was denied to execute command ps -e	ps	IP
2011-03-24 17:10:25.0	10.80.65.105	10.80.65.105	HP-UX	B.11.11	sh	root	root	root	reject	<W> User root:0(10.80.65.105) was denied to execute command awk {if (index($4, "psmctd")) print $1} -	awk	IP



Reti_Login UID_Details

Start Date: 2011-03-16 00:00:00 End Date: 2011-03-31 00:00:00
Aliases: OFF LoingUserID: LIKE root

Occured at	Source IP	Server IP	OS	OS version	Process name	Login user ID	Effective User ID	Real User ID	Message type	Message	Object	Protocol
2011-03-16 16:13:24.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	cmmd	root	root	root	config	Security option policy was modified	/usr/src/cmm/data/config/pv.option	IP
2011-03-16 16:14:01.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	cmmd	root	root	root	config	Security option policy was modified	/usr/src/cmm/data/config/pv.option	IP
2011-03-16 16:15:00.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	cmmd	root	root	root	config	Security option policy was modified	/usr/src/cmm/data/config/pv.option	IP
2011-03-16 16:27:03.0	10.80.18.240	127.0.0.1	RedHat Linux	2.6.18-128.el5	bash	root	root	root	reject	<C> Supervisor was denied to login from remote host	/bin/bash	IP
2011-03-16 16:27:03.0	10.80.18.240	10.80.71.200	RedHat Linux	2.6.18-128.el5	sshd	root	root	root	login	Login succeeded	sshd	IP
2011-03-16 16:27:03.0	10.80.18.240	10.80.71.200	RedHat Linux	2.6.18-128.el5	sshd	root	root	root	logout	Logout	sshd	IP
2011-03-16 16:27:23.0	10.80.18.240	10.80.71.200	RedHat Linux	2.6.18-128.el5	sshd	root	root	root	login	Login succeeded	sshd	IP
2011-03-16 16:27:23.0	10.80.18.240	10.80.71.200	RedHat Linux	2.6.18-128.el5	sshd	root	root	root	logout	Logout	sshd	IP
2011-03-16 16:29:23.0	10.80.18.240	10.80.71.200	RedHat Linux	2.6.18-128.el5	sshd	root	root	root	login	Login succeeded	sshd	IP
2011-03-16 16:29:23.0	10.80.18.240	10.80.71.200	RedHat Linux	2.6.18-128.el5	sshd	root	root	root	logout	Logout	sshd	IP

系統強固與安全

提供系統強固 B1 安全等級的保證，所有的傳輸資訊與儲存資料完全加密。

作業系統支援列表

作業系統	版本	Retie Shield	SecoureOS	PAM
Solaris	5, 6, 7, 8, 9, 10	Yes	Yes	Yes
AIX	4.3X, 5L,6.1	Yes	Yes	Yes
HP-UX	11.0, 11.x	Yes	Yes	Yes
Tru64	4.x, 5.x	Yes	Yes	Yes
Linux	2.2.x, 2.4.x, 2.6.x	Yes	Yes	Yes
UnixWare	7.x	Yes	Yes	Yes
Windows	2000,XP, 2003,2008	Yes	Yes	

註： 支援虛擬系統(Virtual System)

效能參考

測試軟體： 以LoadRunner 7.80版本測試

測試平台： HP伺服器並執行SAP應用程式與DBMS資料庫系統

	Retie Shield Unloaded		Retie Shield loaded		Degradation rate	
No. of times	Total load	Over load	Total load	Over load	Total load	Over load
1st	3.797	5.156	3.613	4.557	4.85%	11.62%
2nd	3.617	4.439	3.569	4.356	1.33%	1.87%
3rd	3.464	4.202	3.557	4.458	-2.68%	-6.09%
Average	3.626	4.599	3.580	4.457	1.2%	2.5%

註：TPS Measurements