



Port- and device control

Krijg weer controle over de end points binnen het netwerk

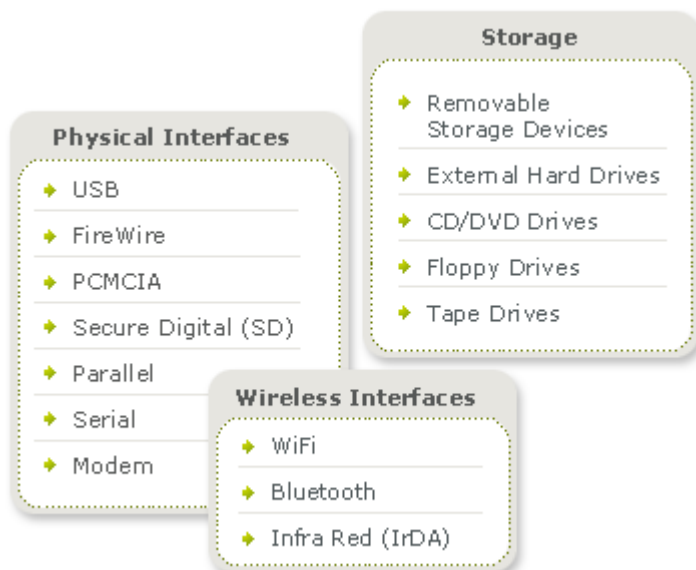
-port- en device control

-Harddisk encryptie



Safend Protector is de meest uitgebreide, veilige en gemakkelijk te gebruiken end-point DLP (Data Leak Prevention) oplossing. Het geeft controle over elk end-point, elk device en over elke interface op de PC en of laptop.

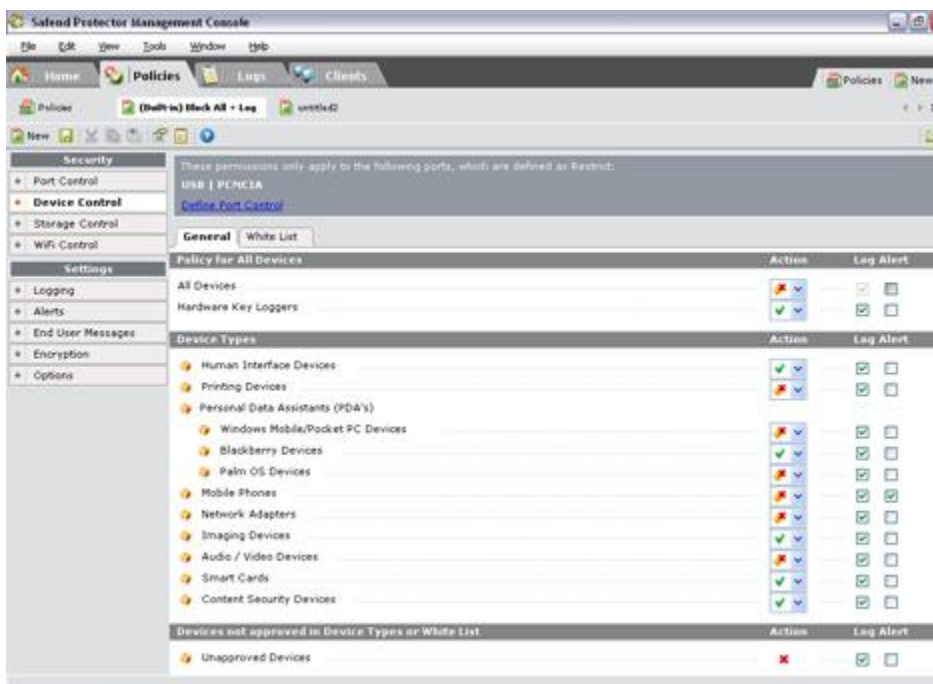
Safend Protector monitort in real-time verkeer wat via de end-points het netwerk in- en uitgaat. Het stelt klanten in staat om een fijnmazige security policy te maken die controle geeft over alle fysieke poorten (USB, Serieel etc). Maar geeft ook controle over data die van en naar opslagmedia gekopieerd wordt. Ook is het mogelijk om de draadloze interfaces (Bluetooth, Infrarood etc) te controleren.



Safend Protector detecteert randapparatuur die op de PC's wordt aangesloten. Safend maakt het vervolgens mogelijk om gebruik van aangesloten apparaten te beperken of te controleren. Men kan hier denken aan beperking op basis van type apparaat, model of zelfs op basis van specifieke serienummers van aangesloten apparaten. Voor opslag media biedt Safend mogelijkheden tot het volledig blokkeren of voor read-only of voor het encrypteren van data die naar opslagmedia gekopieerd wordt. WiFi controles zijn gebaseerd op het MAC-adres, SSID, of netwerkbeveiliging niveau van aangesloten apparatuur.

Controle zonder compromis door voor gebruikers transparante- en niet aan te passen software agent.

Safend Protector maakt gebruik van zeer lichte en fraudebestendige agent software. Deze kan makkelijk op afstand geïnstalleerd worden heeft geen reboot nodig om te werken. De Protector agent werkt op kernel nivo en biedt permanente controle over de end-points. Zelfs local administrators kunnen de security policy niet omzeilen. De agentsoftware is voor gebruikers volledig onzichtbaar tot het moment dat de voorgeschreven security policy overtreden wordt. Op dat moment zal de gebruiker een melding gaan zien. Dit kan bijvoorbeeld wanneer de gebruiker data naar een iPod aan het wegschrijven is terwijl de policy dit niet toelaat.



Safend Protector voordelen.

Fijnmazige controle – detecteert en verbiedt data transfers op basis van apparaat type, model of zelfs uniek serienummer.

Flexibiliteit – policies kunnen gemaakt worden voor elk domein, goep, computer of gebruiker. Koppelingen naar Active Directory of Novell OU's zijn gemakkelijk te realiseren.

Data Awareness- policies op basis van file (type) transfers naar externe storage devices zijn mogelijk. Men kan hier kiezen om dit te blokkeren of toe te staan maar dan wel gebruik te maken van encryptie van de data.

Data bescherming – beschermt data die naar buiten gaat door encryptie toe te passen op data die naar externe drager gaat. Safend protector stelt beheerder ook in staat om gebruik van offline data te tracken.

Eenvoudig te managen - Integreert met Active directory en gebruikt in tegenstelling tot concurrentie een zeer makkelijk te gebruiken en “lichte” management interface.

Tamper-proof – Agent software werkt op kernel-level, geeft real-time analyse van poort verkeer. Agent software is transparant voor de gebruiker en ook daar gebruikers met administrator rechten niet te beïnvloeden.

WiFi Control – gebeurt op basis van MAC address of SSID. Het voorkomt hybrid network bridging door het blokken van WiFi, Bluetooth, Modems of IrDA poorten als de PC verbonden is het corporate LAN.

Anti Hardware Keylogger – blokkeert zowel USB als PS/2 hardware keyloggers.

U3 en Autorun Control – verandert U3 USB drives in “normale” USB drives wanneer ze verbonden zijn met het corporate LAN. Beschermst tegen gevaarlijke auto-launch programma’s door het blokken van autorun.