如何解决公司网络安全及监管问题？

电脑和网络是政府、企业、其它各种组织办公的必需组成部分，帮助各机构大幅提高了工作效率。同时，信息安全、网络行为管理、敏感信息管理等问题成为困扰我们的附骨之蛆：

1、通过 MAIL、FTP、BBS 等途径私自发送公司的财务、销售、设计图纸等公司机密给外人，未加控制的高效网络泄密通路！

2、大多管理员都遇到过这样的情况，明明发现了某个 IP 的计算机做了一些违规的事情，但就是找不到它！

3、销售随意存取读写设计图纸、离职员工访问公司财务资料---------无权限的访问控制是祸根！

4、局域网中某台机器感染某些蠕虫病毒后,造成网络局部阻塞、瘫痪！

5、员工或外来人员将笔记本、PDA、移动硬盘、U 盘等终端存储、通讯设备带入公司，随意窃取机密文件；

6、员工的工作外网络行为：

玩：玩单机游戏、网游、上无关网站、聊天、听歌、看电影、狂下载、还有网络电影电视等；

私活：做私单、投简历找工作、学插花、整 QQ 空间、；

泄密：进入公司电脑、服务器获取非授权的机密资料，随意拷贝资料到自己的存储介质等。

7、IT 资产越来越多、越来越复杂、运维成本也越来越高，真正使用状况如何，无从分析：

例如：

终端越来越多，无法集中管理，软、硬件资产无法确实掌握，盘点、管理困难；

员工私装软件，I P 随易变更，造成故障频传；

软、硬资产私下挪用窃取、非法拷贝、资料外泄，无法监管，造成公司财产损失；

因此：

1、网内的非法外联是网络安全的极大漏洞，如何发现，如何控制，以保证局域网的边界安全？

2、IP 地址盗用、随意变更、私装软件是网管员最头疼的问题，当几十台、几百台、几千台终端联网，如何管理、如何控制？

3、越来越多的外来存储设备（如外来的笔记本、PDA、U 盘、移动硬盘等计算机设备、手机等通讯设备等）擅自接入公司内部网络的情形，如何管理、控制这些潜在的风险？

4、网络流量突然增加，如何快速得知来自网络中的具体位置，如何控制该端口？

5、如何管理越来越多的 IT 资产？

6、如何保护公司的财务、销售、设计、生产、客户等机密资料？

7、如何监管局域网、因特网的员工行为，以便更有效的提高工作效率？

……

如何方便、便捷、有效、可呈现的解决这些问题？答案是：

Heimdall网络可信综合防护平台

系统特点

界面清晰、操作简单的平台系统

实用、方便、高效的实时检测

全方位的日志记录、图表化的分析查询

丰富、客制化的集成接口，与多种软件紧密结合，提供卓越的二次开发支持。

系统功能

1、证书及密钥管理子系统

为平台提供密码配置、公钥证书和传统的对称密钥的管理等密码服务。通过基于国密局认证的硬件密钥技术和军工密码技术发放硬件密钥、同时执行身份控制和访问控制，以确保安全。

由证书管理系统、密钥管理系统、证书审核系统以及相关服务器等相关部分组成。此子系统为平台提供密码配置公钥证书和传统的对称密钥的管理等密码服务。公钥证书采用标准的 X.509 标准，全面支持 X.509 V3 证书类型和标准定义的扩展系统支持 X.509 V2 证书撤销列表(CRL)，确保认证基础以及最好的兼容性。此子系统提供以下管理证书的方式：注册、审核、签发、撤销、发布、备份和恢复， 建立对称密钥管理平台对对称算法密钥进行管理：产生、分发、备份和恢复。

此子系统还为二次开发提供接口支持，根据应用开发商的要求提供支持网络身份认证和访问控制服务的标准 C 语言接口、Java 接口、ActiveX 控件，还可提供包括：CSP、PKCS#11、NOTES API 等各种形式的接口，有效的支持强扩展。

本子系统是平台对对称密钥、用户加密密钥的产生及管理的机构，主要完成密钥的产生、分发、存档、备份、更新、恢复、销毁等功能。支持查询、存储密钥历史档案、系统日志记录管理等功能。

本子系统还提供了基于 PKI 体系的认证模式的身份认证与管理体系，采用软硬件相结合一次一密的强双因子认证模式，将密钥及证书保存在智能密码密码模块中，很好地解决了安全性与易用性之间的矛盾。

智能密码模块是通过国家密码管理局（原国家密码管理委员会办公室）安全性审查的客户端加密产品，可存储标志持有者身份、持有者权限等非常敏感、重要、保密的信息，如数字证书的公钥、私钥。自带有密码运算的加密协处理器，保证密码运算的安全性和高效性。除此以外，智能密码模块无需借助读卡器，可通过 USB 接口直接与计算机相连，使用非常方便。