某保险公司安管平台案例介绍

SOC 事业部

网御神州科技有限公司

- **客户问题**

该保险公司网络由总公司核心数据区、对外服务区、总公司办公区、各个地市分局办公区局域网，以及分布在各地的保险社共同组成。之前，该公司 IT 网络中已经部署了大量的网络设备、安全设备和应用系统，例如防火墙、入侵检测（IDS）、数据库系统、中间件系统以及各种应用系统等，而且选用的网络和安全设备厂家和品牌也比较多，包括思科、IBM、网御神州、港湾等不同厂家的多种型号产品。复杂的网络和设备环境，给该公司的 IT 管理人员带来了沉重的工作负担，耗费了大量时间用于网络故障的定位和排查，网络运行的可靠性保障受到了极大的挑战。

与此同时，随着 IT 网络搭建成形和大量应用信息系统相继上线，公司整个网络的信息系统面临的各种安全风险也日益严重。如何确保信息系统安全运行和信息化的健康发展，成为公司信息系统建设过程中面临的一个主要问题。公司迫切需要一套稳定成熟的安全管理系统，把重要的信息系统统一监控和管理起来。

- **项目实施**

通过招标，该公司最终选择网御神州 SecFox-SNI 安全网络监控系统为其提供全面的网络和信息系统统一监控和管理手段。

SecFox-SNI 采用统一的管理平台集中、实时地监控网络安全状态，对包括路由器、交换机、IDS（入侵检测）、各厂家的防火墙以及各种服务器等在内的网络设备进行统一管理，解决了安全管理过程中分散、非实时的问题，实现了统一、协调管理，大大地提高了该公司 IT 管理人员的工作效率。

SecFox-SNI 除了具备传统的网络管理功能之外，同时还提供了安全审计的功能，对防火墙日志和其他设备的 syslog 进行处理和审计，协助 IT 管理员及时发现该公司网络的安全隐患和薄弱环节。

SecFox-SNI 提供了统一的窗口，可以以表格和多种图形方式，同时监控来自多台设备的安全事件，方便网管人员的管理。除此之外，SecFox-SNI 还可以自动进行 7×24 小时的预警，对高风险的事件通过控制台、短信、邮件多种形式及时通知管理人员。通过 SecFox-SNI 对一段时间内各种网络安全告警的统计，帮助该公司提前做出安全防御准备或者动态地调整安全策略，并为事后安全审计提供依据。

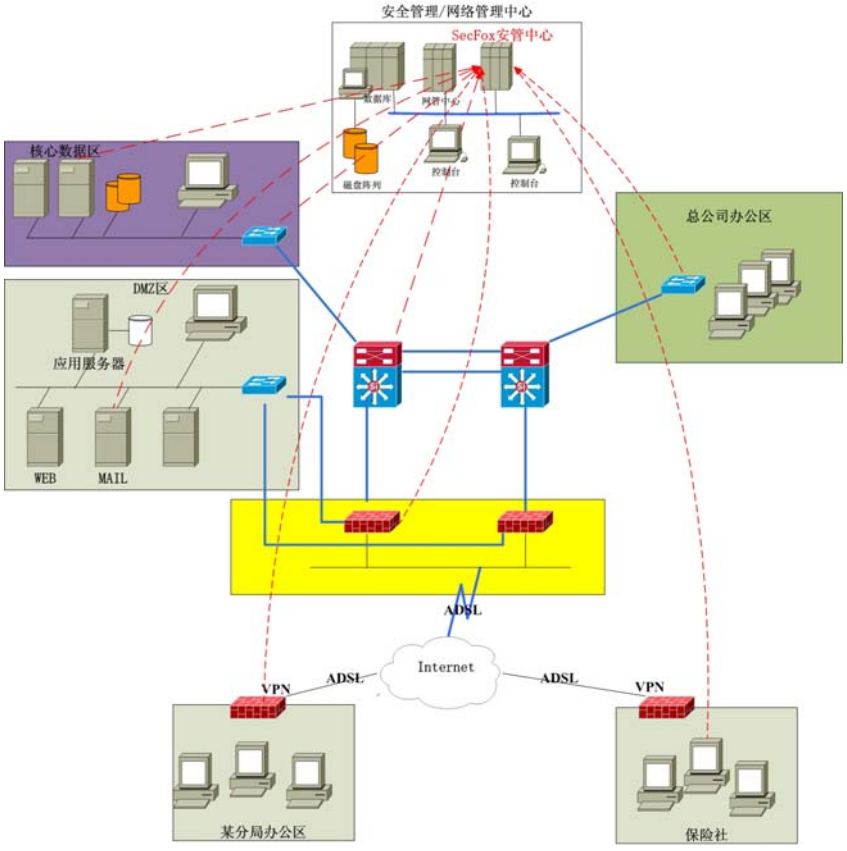
SecFox-SNI 不但能够管理各类网络设备，而且能够管理该公司的各类应用系统和业务系统，提供真正的全方位的管理，管理的应用系统包括数据库、中间件、邮件系统、web 服

务、应用服务，等等。管理员在一个统一的管理平台集中监控各类网络节点和应用系统，全方位的监控企业的 IT 环境，防患于未然。

- **客户价值**

通过部署 SecFox 安全管理系统，该公司有效实现了对现有的各种安全和网络设备的资源整合，动态协调和管理现有的 IT 资源，发挥它们应有的作用。同时，在维持现有人力资源的情况下，使安全管理人员全面实时地掌握系统内的安全状况，及时地发现安全风险和事故，并进行及时地处理，减少安全事故造成的损失。

在成功实施 SecFox 安全管理系统的基础上，网御神州还为该公司提出了建设综合性安全管理平台的二期目标和方案。借助网御神州贯穿安全咨询与服务、安全管理系统和安全硬件设备的整体安全解决方案，该公司正在逐步落实全面可控安全体系建设的构想。



欲获取更多信息，请即联系网御神州科技（北京）有限公司

全国统一热线服务电话：010-87002000（7×24 小时）

E-mail：service@legendsec.com（5×8 小时）

网站地址：www.legendsec.com

网神安全管理博客地址：http://blog.sina.com.cn/legendsec

传真：010-62972896

通信地址：北京市海淀区上地信息产业基地开拓路 7 号先锋大厦 2 段 1 号

邮政编码：100085