# 中国企业信息安全解决方案

## 发展趋势分析报告

# 目　　录

# 一、企业信息安全现状

## 1、企业信息安全威胁现状

企业科技专业人士对企业的信息安全正越来越迷惘。一方面，企业不断加大在信息安全方面的投入，但与此同时，他们又认为自己的企业更加脆弱，更加容易受到攻击。本报告针对企业级信息安全解决方案和信息安全产品用户，以数据和图表向读者展示当前企业信息安全的现状、企业对信息安全的投资现状以及信息安全市场的趋势分析，并希望通过切实可行的信息安全实施建议，为企业在信息安全解决方案上的实施提供支持。

近两年来，中国企业信息系统用户的信息安全意识已经普遍得到提高，尤其是金融、电信、民航、电力、制造业等信息化程度高的重点行业，已经开始广泛部署各种网络安全技术和产品，然而，目前的安全形势依然不容乐观，病毒、木马、钓鱼攻击、垃圾邮件、僵尸网络、间谍软件、恶意软件、针对漏洞的攻击等依然会以各种不同的面貌出现，也不排除会出现新的攻击形式。据统计，2007 年电脑感染病毒的比例高达 90.8%，其中电脑感染次数达五次的比例为 35.8%；而账号/个人信息被盗、被改的则接近 45%，其中账号 / 个人信息被盗 1－2 次的更高达 63.2%。此外，仅 2007 年上半年我国被植入木马的主机 IP 就增长了 21 倍。除了恶意软件大幅度增加之外，2007 还出现了暴风蠕虫，它是一系列后门木马和电子邮件蠕虫的统称，这些木马和蠕虫共同创建了大规模的分布式点对点僵尸网络。同时，入侵数据库的行为在 2007 年危害巨大，大量企业和政府的敏感数据被窃取。

IBM 一份专门针对中国企业安全性的调查显示，有 38%的中国企业已经意识到，信息安全比实际犯罪对他们的业务更具威胁，企业的品牌和声誉很容易因此造成严重的损失。而当前被报道的案例只是整个遭受安全损失的企业的冰山一角，更多的企业出于对企业形象的考虑，而没有对外声明自己被攻击的事实以及攻击带来的实际损失。

对于企业用户而言，过去的问题更多的是关于病毒和蠕虫，同时它们现在也仍然存在。当今更大的挑战在于间谍软件、入侵防护系统、网络欺诈和网络犯罪，这些是不能仅靠技术就可以解决的。从表面上看，病毒和蠕虫依然猖獗，但各种攻击手段的不断混合，使得企业面临不断变化着的安全环境和不断加剧的威胁，这正是企业大量投入信息安全建设却仍然无法得到安全感的原因所在。依据企业信息安全威胁的来源，可以分为来自企业外部的威胁和企业内部的威胁两大类。

### 1）企业外部信息安全威胁

企业外部信息安全威胁在形式上包罗了当前信息安全的各种形式，如病毒、木马、蠕虫、恶意软件等。据市场研究组织 Webroot 的最新统计，中国约有一半的企业遭受了恶意攻击，有组织的恶意攻击呈上升趋势。调查还发现，有 40%的企业称因各类恶意软件攻击而受到了不同程度的损失，是比例最大的一部分；有 26%的企业称，公司的机密信息被恶意软件盗取；有 39%的企业宣称经常受到特洛伊木马的攻击；另有 24%的企业则称，经常受到系统性监控攻击；有 20%的企业受到键盘记录式攻击。如图：“企业安全状况调查情况”所示。

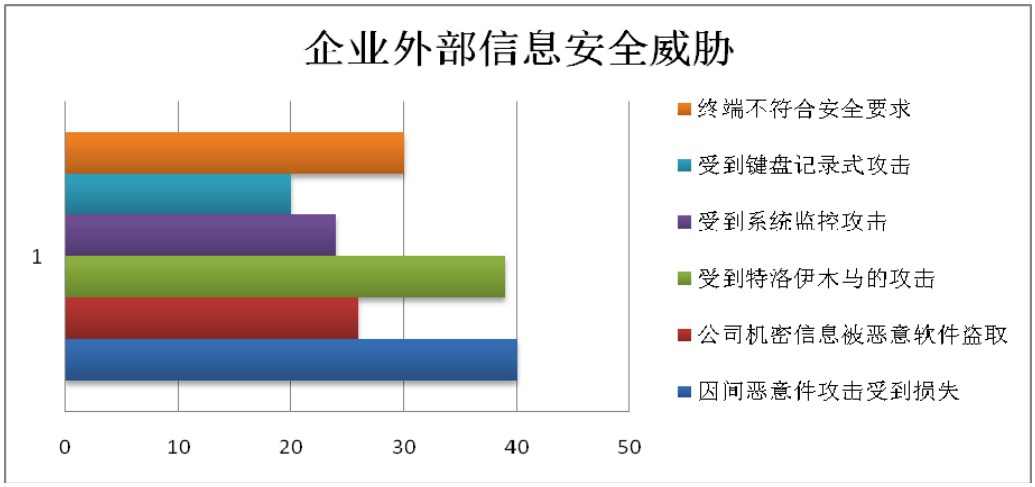


图 1 ： 企业外部信息安全威胁

另据《信息周刊》和埃森哲咨询公司合作进行的 2007 年“全球信息安全调查”提供的数据，针对中国和美国企业进行的调查中，在回答企业信息安全在哪些方面比去年更严重的问题上，具体数据如下图所示：

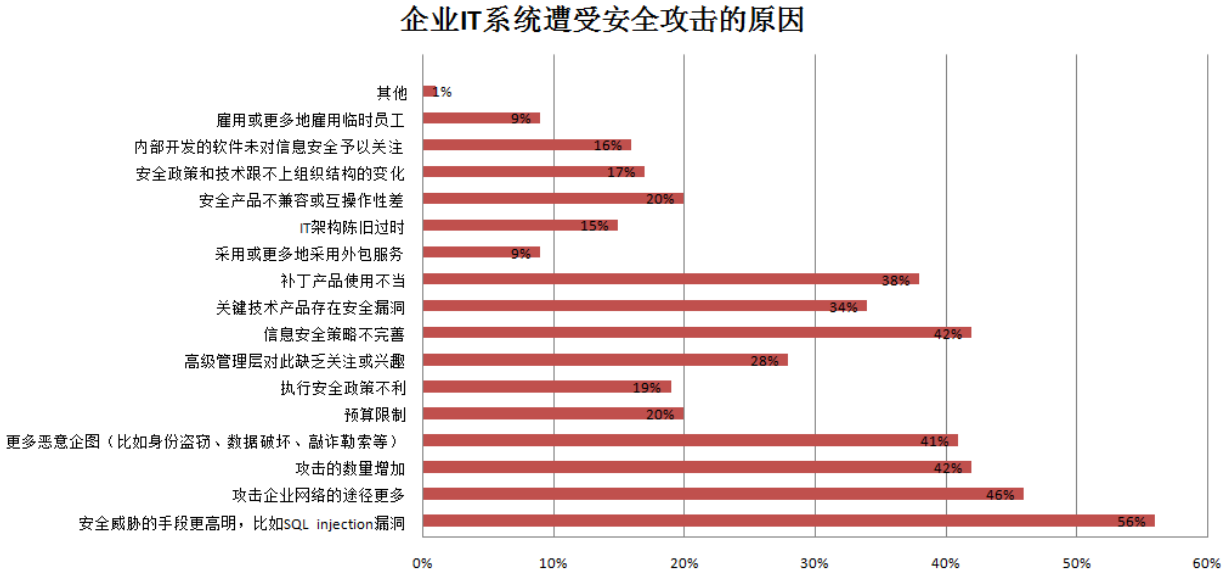


图 2 ： 企业 IT 系统遭受安全攻击的原因

在 2007 年，对信息安全威胁最大的是恶意软件，相应的传播恶意软件的网站也占据了 2007 年信息安全威胁的主导地位，依据 Gartner 的统计数据，中国以 32.95%的恶意网站数量居排行榜首位，美国以 25.90%紧邻其后，这两个国家在近几年相关的恶意软件统计中几乎一直占主导地位，要改变排名先后取决于恶意软件编写的趋势和操作系统的发展。在中国最流行的恶意软件载体是被黑网站和所谓的“防弹主机”，在美国，主要是被黑客攻击“.com”网站和一些利用窃取的信用卡购买到的合法主机资源。 俄罗斯和巴西占据第三和第四位。这些国家情况类似，因为大多数恶意程序托管在“免费主机资源”中，网络服务提供商为用户提供机会可以向计算机上传自己的网站。

下图为使用 Akross 系统检测到的传播恶意软件 IP 地址地理分布图：

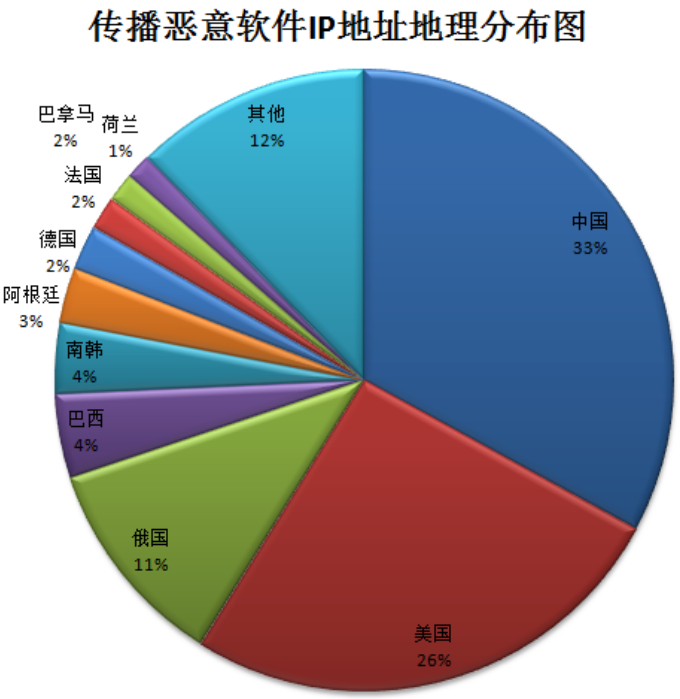


图 3 ： 传播恶意软件 IP 地址地理分布图

通过分析以上数据，报告认为在未来 3-5 年内，上述威胁状况及所占的比例并不会发生根本性的变化，传统的威胁方式将持续存在，同时无法避免新的威胁形式出现。因此在未来的 3-5 年内，企业将面临更为严峻的外部安全威胁形式。

## 2）企业内部信息安全威胁

在图 1 中，有 30%的企业同时存在由于终端不符合安全要求带来的安全问题，这类安全问题往往来自企业内部，有最新的统计显示，企事业核心数据的流失实际上有 80%左右源于企业内部人员的不正当行为，而只有约 20%来自外部的侵犯。近来频频发生的因内部网络安全导致的商业情报失窃事件，如韩国起亚“索兰托”泄密事件等，也进一步证实了这种观点，并改变着安全管理人员的观念。 因此，如何保护企业的信息资产，如何防范内部人员犯罪，发生信息泄漏事件之后如何进行取证已经成为今后信息安全建设的一个重要部分。

依据国家计算机应急响应中心发布的数据，在所有的计算机安全事件中，约有 52%是人为因素造成的，25%由火灾、水灾等自然灾害引起，技术错误占 10%，组织内部人员作案占 10%，仅有 3%左右是由外部不法人员的攻击造成。如图 4 所示。

简单归类，属于管理方面的原因比重高达 70%以上，而这些安全问题中的 95%是可以通过科学的信息安全管理来避免。因此，管理已成为信息安全保障能力的重要基础。安全管理（SM），已经成为企业管理（EM）的一个重要组成部分。从信息管理的角度看，安全管理涉及到策略与规程，安全缺陷以及保护所需的资源，防火墙，密码加密问题，鉴别与授权，客户机/服务器认证系统，报文传输安全以及对病毒攻击的保护等。

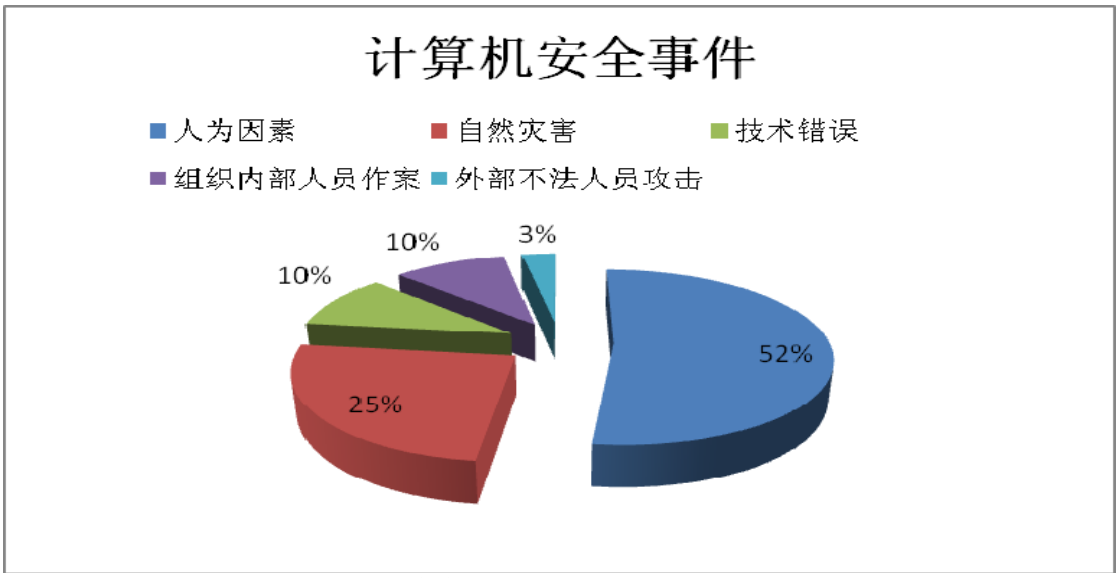


图 4：计算机安全事件发生因素统计结果

除此之外，依据“全球信息安全调查”的数据，中国企业在应对企业内部带来的安全隐患问题上，将面对以下安全挑战：

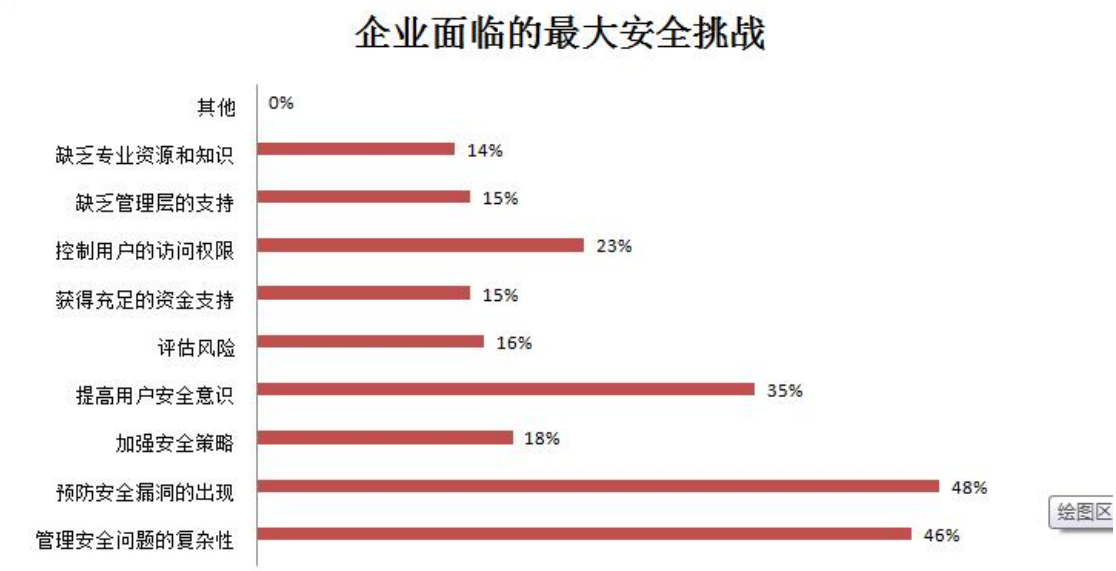


图 5 ：企业面临的最大安全挑战

实际上，安全管理不是一个简单的软件系统，也不能单纯地通过企业的信息部门来解决，它包括的内容非常多，主要涵盖了安全设备的管理、安全策略管理、安全风险控制、安全审计等几个方面。它主要解决以下问题：集中化的安全策略管理（CSPM）、实时安全监视（RTSA）、联动机制（CM）、配置与补丁管理（CPM）、统一的权限管理（PMAE）、设备管理（DM）在具体的实施上，需要整个企业从上到下的统一的策略制定和执行，以及相应的信息安全意识培训，来提高整个企业的安全管理意识，从而保证企业的信息安全性。

## 3）信息安全威胁给企业带来的损失

依据《信息周刊》和埃森哲咨询公司合作进行的 2007 年“全球信息安全调查”提供的数据，对企业在过去的一年里遭受的信息安全攻击所占比例的统计如下图所示：

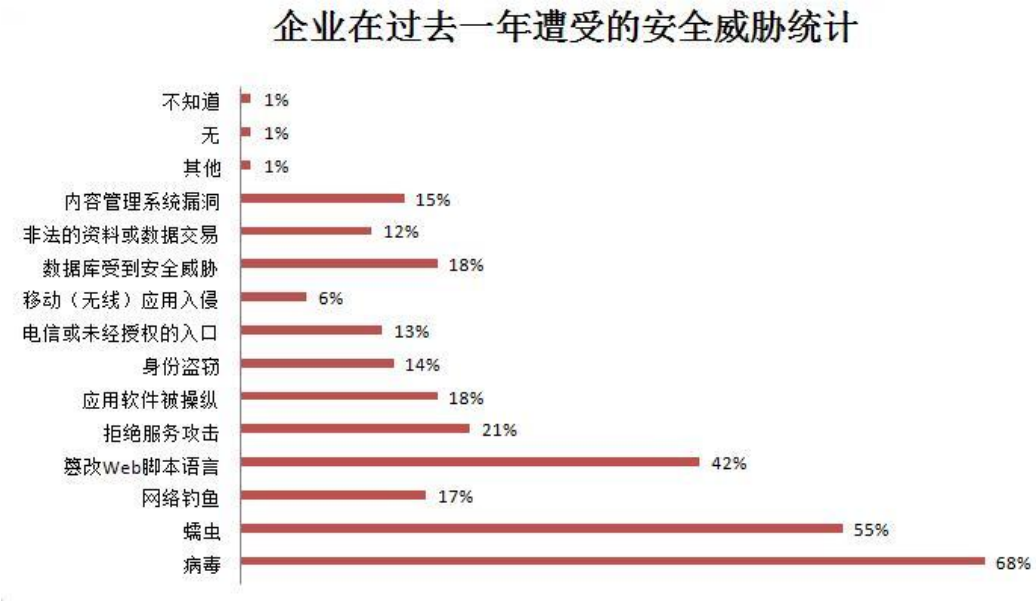


图 6 ： 企业遭受的安全威胁统计

从上图中可以看到，传统的病毒、蠕虫、修改 Web 脚本语言和拒绝服务攻击为比例最高的四项，在今后相当长的一段时期内，这样传统的威胁将持续存在并将带来不可估量的损失。

对于图 2 中的信息安全攻击行为对企业造成的后果，如下图所示：

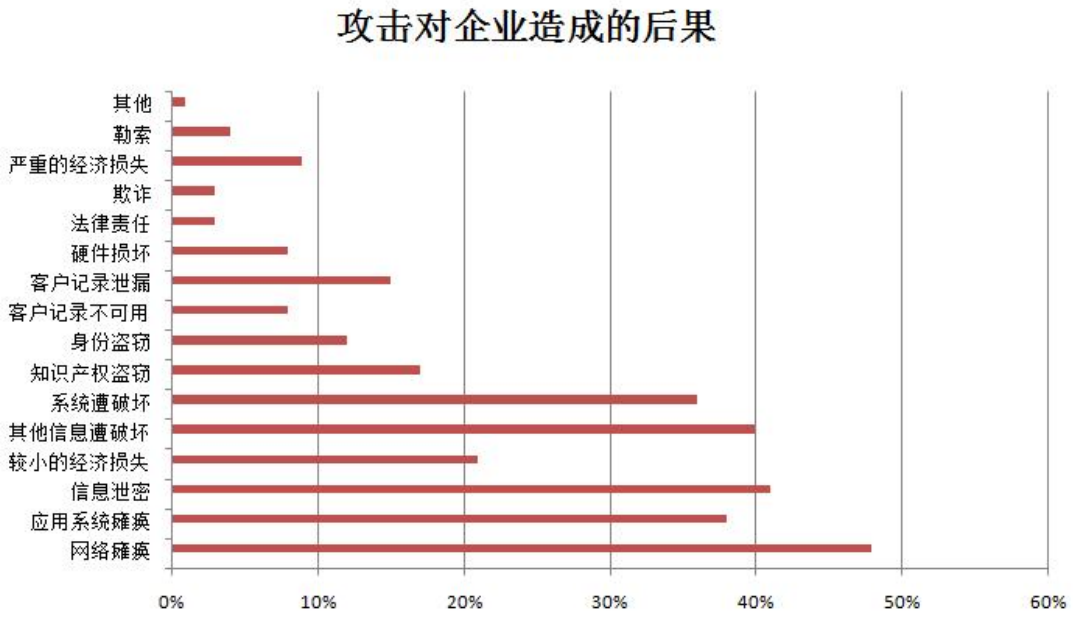


图 7 ： 攻击对企业造成的后果

其中，造成网络瘫痪和信息泄密的事件所占的比例最高，更有近 10%的受调查企业声称遭受了严重的经济损失。随着企业对信息化依赖程度的增高，信息安全威胁带来的威胁将会呈现持续增高的趋势，而且在越来越多的情况下，这些威胁将直接导致企业经济上的损失。

## 2、企业信息安全投资现状

在经历了数年的企业信息化投资和整个高新技术产业的发展之后，中国已经拥有相对完善的通信基础架构，很多大中型企业也拥有了比较完善的企业信息系统以及整体的 IT 基础架构，其中包括采用不同层面的安全解决方案。在引入新的、更能优化企业流程、推动企业效益提高的 IT 解决方案之前，绝大多数企业希望现有的 IT 投资能够继续发挥作用，同时企业还希望能够降低 IT 部门的运营成本，以进一步提高企业利润。

在对 120 家国有重点企业、120 户试点企业集团和地方重点企业的信息化调查中显示，我国企业对信息化建设的重视程度进一步提高，其中 83.3%的企业设立了副总裁、副总经理级的信息主管；89.7%的企业建立了专门的信息化领导管理机构；94%的企业已经制定、正在制定或计划制定企业信息化总体规划；77.4%的企业建立了统一的信息管理制度；80%的企业制定了“十五”信息化建设投入预算；89.1%的企业设有专职信息系统管理和维护人员；86.7%的企业根据技术发展和业务需求适时进行系统改造和升级；74.9%的企业把“信息化人才培训”列为工作重点。

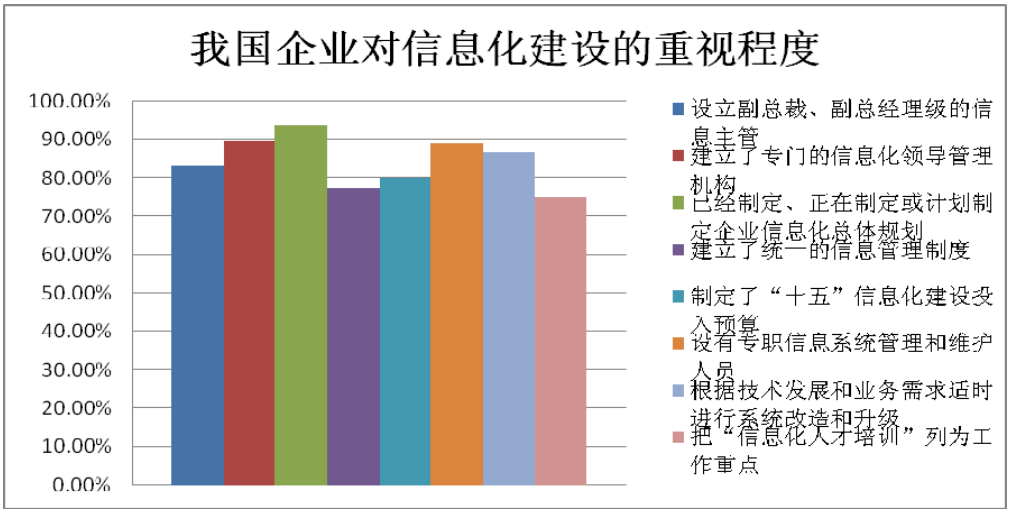


图 8：我国企业对信息化建设的重视程度统计图

与此同时，我国 96%的国务院部门、所有省级政府、98%的地市级政府、83%的县级政府建立了政府网站。金税工程使全国增值税征收率从 2000 年的 61%提高到目前的 86%；金保工程使养老金核对发放时间由 3 个月减少为 3 天。企业信息化水平明显提升，网上采购商品及服务的比重超过了 13%。

在网络安全的 IT 投入上，无论是电信、银行行业，还是汽车、家电等制造行业，盛行的都是认为内部网络、外部网络安全投入的合适比例为 2：8，即“2：8 法则”，普遍存在重外轻内的现象。当前内部网络安全事件之所以层出不穷，主要是由于企业 IT 管理人员受对内部网络安全的重视不足、投入过少。而企业的 IT 人员对内部网络安全的认识存在误区，即简单地认为内部网络安全就是监控审计，或者内部网络安全就是数据加密，这种观念使建立起来的内部网络安全体系或多或少都留有隐患；内部网络安全体系还涵盖身份认证、授权管理等方面，需要一个功能强大、应用覆盖面广的平台方能胜任。同时市场上缺乏成熟的内部网络的安全解决方案，也使得许多企业无法采购到符合实际应用需求的相关产品。

首先分析企业信息安全涉及的方面，如下图所示，企业内部网络的安全和管理主要涉及：内部信息系统安全的防护，包括虚拟专用网络（VPN）、多层防火墙、多方位入侵监测与预防机制、基于多种协议的防病毒软件、反间谍软件（Anti-Spyware）、反钓鱼软件（Anti-Phishing）、反垃圾邮件（Anti-Spam）以及网页过滤等技术；内部员工电脑操作行为的规范；内部电脑使用情况的监管；企业信息资源的管理与集成；日志记录与取证。


图 9：企业内部网络安全解决方案

依据“全球信息安全调查”的数据，在未来一年内，受调查企业将在以下方面采取相应的安全措施，具体比例如图 10 所示：

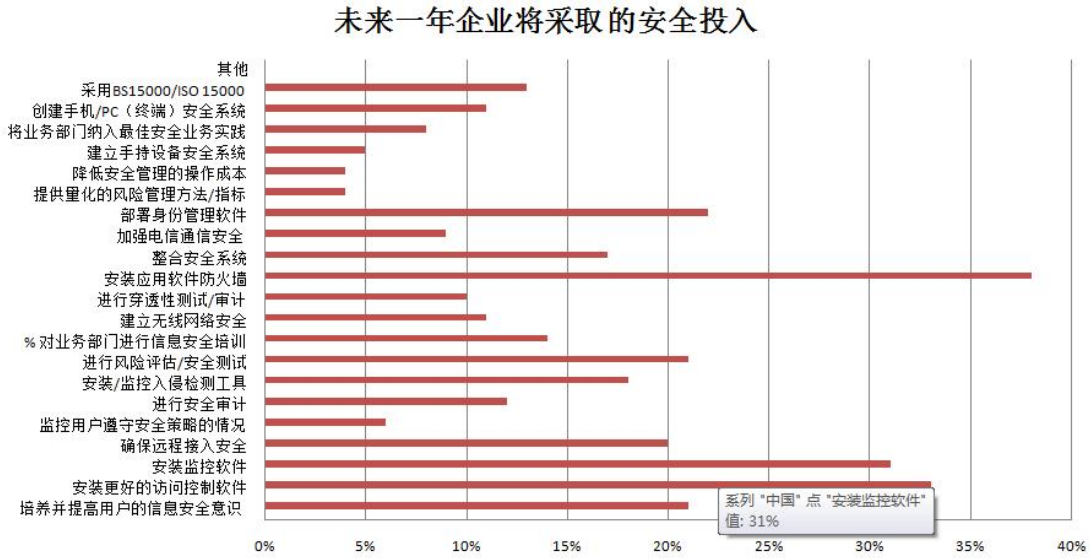


图 10 ： 未来一年企业将采取的安全投入

# 3、企业现有安全产品分类

当前中国大多数企业采用的安全产品属于传统的安全产品，与全球整个信息安全行业安全产品现状和发展趋势相比，仍存在较大差距，报告对当前大多数企业采用的安全产品进行归类和说明。

当前中国解决网络信息安全问题的主要途径是利用密码技术和网络访问控制技术。密码技术用于隐蔽传输信息、认证用户身份等。具体解决方案和产品大致可以分为以下几类：

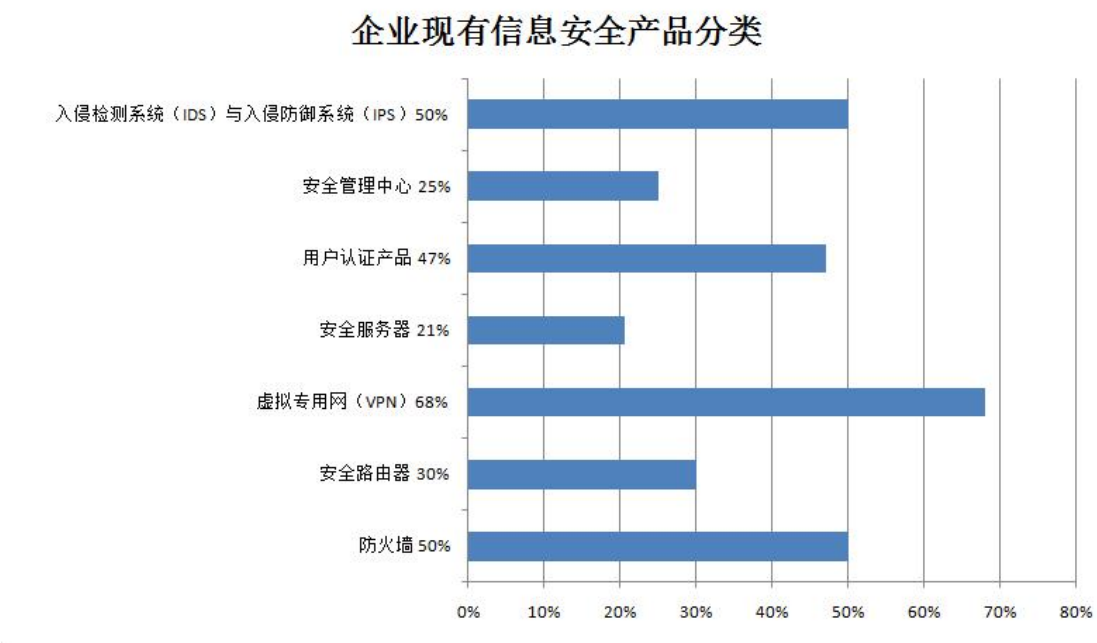


图 11 ： 企业现有信息安全产品分类

## 1）防火墙

防火墙在某种意义上可以说是一种访问控制产品。它在内部网络与不安全的外部网络之间设置障碍，阻止外界对内部资源的非法访问，防止内部对外部的不安全访问。主要技术有：包过滤技术，应用网关技术，代理服务技术。防火墙能够较为有效地防止黑客利用不安全的服务对内部网络的攻击，并且能够实现数据流的监控、过滤、记录和报告功能，较好地隔断内部网络与外部网络的连接。但其本身可能存在安全问题，也可能会是一个潜在的瓶颈。

## 2）安全路由器

由于 WAN 连接需要专用的路由器设备，因而可通过路由器来控制网络传输。通常采用访问控制列表技术来控制网络信息流。

## 3）虚拟专用网（VPN）

虚拟专用网是在公共数据网络上，通过采用数据加密技术和访问控制技术，实现两个或多个可信内部网之间的互联。VPN 的构筑通常都要求采用具有加密功能的路由器或防火墙，以实现数据在公共信道上的可信传递。

## 4）安全服务器

安全服务器主要针对一个局域网内部信息存储、传输的安全保密问题，其实现功能包括对局域网资源的管理和控制，对局域网内用户的管理，以及局域网中所有安全相关事件的审计和跟踪。

### 5）用户认证产品

由于 IC 卡技术的日益成熟和完善，IC 卡已经被广泛地用于用户认证产品中，用来存储用户的个人私钥，并与其他技术如动态口令相结合，对用户身份进行有效的识别。同时，还可利用 IC 卡上的个人私钥与数字签名技术结合，实现数字签名机制。随着模式识别技术的发展，诸如指纹、视网膜、脸部特征等高级的身份识别技术也将投入应用，并与数字签名等现有技术结合，必将使得对于用户身份的认证和识别更趋完善。

### 6）安全管理中心

由于选用的安全产品较多，且分布在不同的位置，这就需要建立一套集中管理的机制和设备，即安全管理中心。它用来给各网络安全设备分发密钥，监控网络安全设备的运行状态，负责收集网络安全设备的审计信息等。

### 7）入侵检测系统（IDS）与入侵防御系统（IPS）

入侵检测，作为传统保护机制（比如访问控制，身份识别等）的有效补充，形成了信息系统中不可或缺的反馈链。入侵防御系统则是入侵检测系统的升级版本，变被动检测为主动防御，属于市场发展空间较大的产品。

信息安全的解决是一个综合性问题，涉及到诸多因素，包括技术、产品和管理等。目前各大安全厂商开发的防火墙、安全路由器、安全网关、黑客入侵检测系统等产品和技术，主要集中在系统应用环境的较高层次上，在完善性、规范性、实用性上还存在许多不足，特别是在多种平台的兼容性、多种协议的适应性、多种接口的满足性方面存在很大距离。

而对于中国的中小企业而言，企业信息化的道路仅仅停留在功能实现上面，对于解决方案的安全性和重用性，则考虑的不够全面。尤其在安全解决方案上面，采取的是点解决方案，仅针对当前的需求部署一个或片面的几个安全产品，远不能达到企业 IT 投资重用、解决方案集成的目的。

# 二、安全市场发展趋势

## 1、报告核心发现

通过对国内外 IT 研究机构安全报告的研究和安全厂商发布的预测信息，针对安全市场的发展趋势，报告有以下核心发现：

### 1）安全领域仍旧是吸引 IT 专业人员和企业的热点

对于安全人才（包括安全架构师、安全咨询师、安全实施工程师等工作角色）的需求日益增长，企业和个人对不同层面上安全顾问的需求不断增长，而且对于安全人才的能力要求也更高。

### 2）安全解决方案业务收益成为考虑的重点

在制定安全相关决策的时候，决策者越来越多地考虑把重点放在业务收益和投资回报上面，将会有更多的企业采用 ROI、NPV 等模型对企业的安全解决方案的业务收益进行评估。用户希望所采用的安全解决方案能够带来更为实际的经济效益，而不仅仅是一个成本中心。

### 3）用户希望更为集成的安全解决方案

用户希望能够更加紧密地集成到所有的安全产品中去，用户期待能够全面应对当前或以后安全威胁的解决方案，这样解决方案能够全面解决企业安全管理、安全防护以及主动应对不断升级的威胁，最重要的是，用户希望实现这样的解决方案并不需要过于繁琐的配置过程。

## 2、安全市场分类及市场增长分析

依据 Gartner 对安全市场的划分方法，报告把全球范围的安全市场划分为以下三类（如下图所示）：

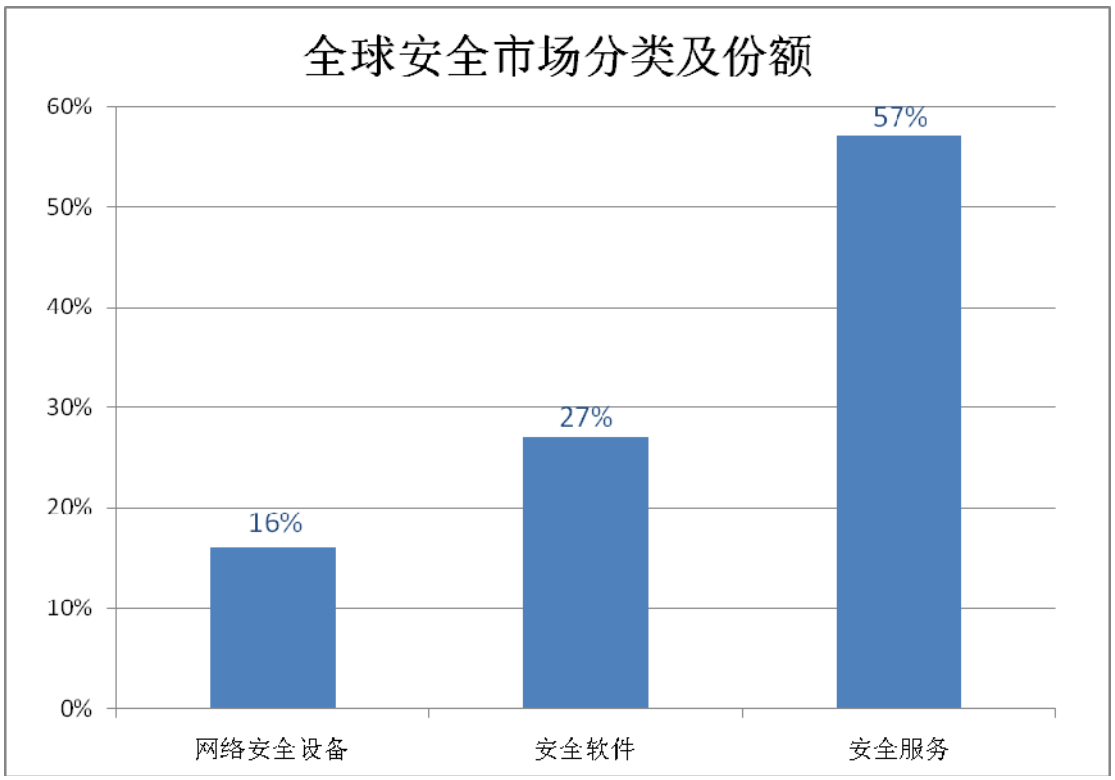


图 12 ： 全球范围的安全市场分类

依据 Gartner 对 EMEA 市场的分析报告，在 08 年企业网络安全设备市场将呈现强劲的增长趋势，数据显示该区域 07 年在这一细分市场上的增长额度至少为 20%；该分析报告还显示，该区域的安全软件市场在 07 年实现了高达 11.5%的增长，达到了 25 亿美元。在网络安全设备市场上，主要的增长来自 IPS 系统和 SSL VPN 两大块，联合和扩展的 IPS 厂商在西欧实现了 07 年增长额为 60%的强劲增长额度，而 SSL VPN 的增长幅度则为 26%。

报告同时指出，在 85%-95%的网络内部，企业内部人员泄密风险是网络安全防范的重点，起到完整的责任认定体系和绝大部分授权功能的审计监控体系对控制来自企业内部人员

风险起到有效的防范作用，是未来安全市场发展的主流。而身份识别、网络隔离、可信服务、防止信息泄漏和备份恢复等产品因为产品细分市场的定位的差别，也会占有一定的市场份额。

对于中国安全市场而言，依据 IDC 发布的《中国 IT 安全市场分析与预测 2007-2011（1H07）》，2007 年上半年，中国 IT 安全市场的市场规模为 3.195 亿美元，同比增长 27.0%。其中安全软件市场在 2007 上半年的市场规模为 8760 万美元，占整体市场的 27.4%；比例最大的是安全硬件，为 48.6%，同比增长 28.3%，市场规模为 1.551 亿美元；IT 安全服务市场占 24.0%，市场规模为 7680 万美元。IDC 同时预计，从现在起的 3～5 年内，信息安全市场将保持高速、超规模的发展势头，尽管增长率变缓，但实际的增长数额强劲。其中电信、政府、金融将会是 2008 年信息安全需求最大的行业。电信业和金融业是投资大、发展快、信息化程度高而需求复杂、安全形势相对严峻的行业，而政府部门则因站位较高、安全需求迫切，对外（包括国内商界和全球政经界）又在时刻发挥着示范作用，所以也会加大对信息安全的投入。

如下图引用的 IDC 预测的 2007-2011 中国 IT 安全市场的规模和增长率示意图。


图 13：中国 IT 安全市场规模（2006-2011 年）

# 3、07 年增长驱动因素

## 1）符合法规性

更多的与符合法规事件相关的考虑、更高的系统可用性和对基础架构的破坏限制，以及业务驱动的更高的利益。

## 2）业务收益驱动

安全市场的增长得益于业务收益的驱动，但是对安全投资基于 ROI 模型的论证是一项

难以避免且难以实施的任务，大多数企业已经开始采用相应的投资回报模型开始评估安全解决方案所能带来的实际收益。

### 3）SMB 投入加大

针对 SMB 市场不断增大的需求，基于联合的和服务提供商的在中小企业业务（SMB）上的投资在逐步增长。

### 4）集成解决方案的驱动

企业用户对于集成的安全解决方案的需求和投资在逐步增加，与安全厂商的多样化的宣传相反，用户更倾向于应用更为集成和可以易于部署、实现的安全解决方案，厂商在软硬件结合、软件集成、IT 安全基础架构集成上的推动拉动了市场的增长。

## 4、08 年市场发展趋势

报告认为各个安全市场领域在 08 年将呈现以下发展趋势：

### 1）安全硬件市场

作为 07 年增长最快的安全领域，安全硬件市场在 08 年将持续保持强劲的增势，主流的安全市场依然需要依靠传统的网络技术支撑，依据 IDC 的研究数据，在 08 年，这一市场的增长率将不会低于 18.3%。

**入侵防御系统（IPS）：**主动入侵防御系统的市场增长率已经远大于被动的防火墙、入侵检测系统的增长，企业用户在考虑企业网络安全设备投资的时候，首选为主动入侵防护系统。报告预计 08 年全球范围内这一市场的增幅将达 22.5%，其中 EMEA 区域的市场比例将继续占整个安全硬件市场的 30%，而北美则不会低于 50%，而其他区域的市场份额也不会低于 20%。

**SSL VPN 设备：**08 年经济的全球化将进一步加深，越来越多的制造类、服务类等劳动密集型企业将更多地在劳动力人工成本低廉的区域进行，扩展的分支办公室和总部之间的连接和通讯将会更多的依赖于基于 SSL VPN 的安全设备，从而这一市场将持续保持高增长。依据 Gartner 的数据，北美安全硬件市场将出现 IPS 和 SSL VPN 平分秋色的场面，08 年超过 2/3 的通过网络开展业务的正式雇员首要的网络接入方式将是 SSL VPN，对于合同工的比例为超过 3/4，而临时工则为 90%以上。

**网络防火墙/安全路由器：**作为必要的网络资源投资，网络防火墙和安全路由器将保持一定的市场份额，但相对于 IPS 和 SSL VPN，其增幅则大大降低，对于 IT 基础设施已相对完善的北美和西欧地区，这部分市场可能出现负增长的趋势。这部分市场的增长将主要出现于非洲、亚洲等 IT 基础设施尚不完善的区域。其中中国中小企业在 IT 安全基础设施上的投入将能够确保这一市场的增长率。

### 2）安全软件市场

依据 Gartner 的市场调研数据，2007 年 IT 安全应用软件市场的销售额高达 91 亿美金，

销售的安全软件中有 53.8%，约为 49 亿美元的销售额属于反病毒软件厂商，如 Microsoft、Symantec、McAfee 等。除传统的针对 ES 防病毒技术以外，认证访问管理和 Internet 网关安全等更为主动的防御应用都呈现了较高的增长趋势。在 08 年，企业安全厂商将继续强调不同产品之间的整合，为客户提供多种应用一体化的中央管理产品，这些产品将以套件的方式提供给客户。

在安全厂商实施整合产品战略的推动下，整个 08 年至 09 年的两年间，为整个桌面系统环境购买一体化整合产品的企业的增长率将达到 20%。尽管相对于安全硬件市场的增幅较小，但随着 IT 基础设施的不断完善，整个安全市场的投资已经开始逐渐由硬件基础投资转移到软件基础投资上来，而企业用户不希望重复硬件基础设施整合的经历，而希望在部署之处即引入整合的安全软件解决方案。

因此，在 2008 年，对于 IT 基础设施已经较为完善的企业，软件领域将成为投资的主要领域。个人用户和企业安全实施人员都希望简化 IT 软件部署的需求成为直接驱动安全软件供应商来提高安全软件的整合度的动力。依据对安全软件市场的分类，将出现以下三种类型的套件以及增强的防病毒能力：终端安全（ES）、认证访问管理（IAW）、Internet 网关安全（IGS）。

三种类型套件及其增强的防病毒能力对照表

| 类型名 | 终端安全（ES） | 认证访问管理（IAW） | Internet 网关安全（IGS） |
|---|---|---|---|
| 功能模块 | 反病毒（反间谍软件、反恶意软件等） | 目录服务 | URL 过滤 |
| | 个人防火墙 | 用户提供 | 恶意代码过滤 |
| | 主机入侵防护 | 工作流 | 敏感信息过滤 |
| | 数据丢失防护 | 认证审计/报告 | 文件类型过滤 |
| | 磁盘和数据加密 | Web 访问管理 | Web 应用程序级别控制 |
| | 网络访问控制（NAC） | | |

表 1 ：三种类型套件及其增强的防病毒能力对照表

**增强的防病毒能力：**

应对不断升级的病毒、恶意软件和间谍软件威胁，安全软件技术领域相应的也会出现新的应对技术，病毒特征识别将会从单纯的终端（客户端）转到服务器端。单纯的防病毒领域将出现以下趋势：

● 客户端防御系统将进一步加强与病毒、恶意软件和间谍软件的对抗能力。这种对抗将随着操作系统安全性的提高以及互联网厂商运营能力的提升趋于平衡；

● 类似“可信认证”的技术将得到进一步的发展，服务端判定将逐步取代本地特征码来实现对病毒、恶意软件和间谍软件的识别、分析、报告和清理；

● 识别恶意行为的智能计算，将逐渐从客户端转向服务端，并且通过服务端的数据收集能力，提高恶意行为的标识、监控、记录和防护。

预计在 08 年，针对以上三种套件和增强的病毒防护趋势推出产品的厂商会逐渐增多，安全软件厂商也将加大对现有分散的安全软件产品的集成力度，以套件方式发布满足客户多方面需求的软件。

## 3）IT 安全服务市场

与近年来的 IT 服务外包模式的快速发展类似，IT 安全服务市场也呈现快速发展的趋势，企业客户在决策和实施 IT 安全解决方案之前，越来越倾向于向专业的 IT 安全公司咨询，或在实施过程中聘请专业安全人员担任实施顾问和员工培训，或直接聘请专业安全人员对企业安全漏洞进行弱点测试。依据 Gartner 提供的数据，安全服务市场占据了 06 年全球安全市场的 57%，并且随着 IT 安全基础投资的成熟，这一比例在未来 5 年内还将持续走高。

预计在 08 年，企业用户对安全咨询、安全实施顾问以及安全开发集成人员的需求将持续增长，随着安全威胁的升级和安全解决方案的提升，专业安全人员要不断提升自己的专业技能以适应新的安全环境。

但与国外成熟的 IT 和 IT 安全服务市场相比，中国的 IT 安全服务市场仍然有着较大的发展空间。

# 三、企业信息安全解决方案发展趋势分析

## 1、企业信息安全架构发展趋势分析

与近年来的 IT 基础架构优化和面向服务架构的 IT 基础架构投资理念相呼应，企业在实施安全解决方案的时候大多开始从整体 IT 安全架构的角度入手。在 08 年安全架构的设计的集成趋势将更为明显，企业将在安全解决方案项目立项之初，便充分考虑其可集成性及可扩展性。

将企业信息安全涉及的因素进行细化，其包括下表所示的五大元素：

| 名称 | 简介 |
|---|---|
| 认证（Authentication） | 任何 IT 设备的使用者可以是人、设备和相关系统，无论是什么样的使用者，安全的第一要素就是对其进行认证。 |
| 授权（Authorization） | 授予合法使用者对系统资源的使用权限并且对非法使用行为进行监测。 |
| 保密（Confidentiality） | 保密是要确保信息在传送过程和存储时不被非法使用者窃取。 |
| 完整性（Integrity） | 信息安全的一个重要方面就是保证信息的完整性，特别是信息在传送过程中的完整性。 |
| 不可否认（Non-repudiation） | 无论是授权的使用还是非授权的使用，事后都应该是有据可查的。 |

表 2 ：信息安全的五大元素

企业信息化的安全架构就是根据信息安全的五大要素，从整体上考虑信息的安全防护问题。企业的信息化安全架构应该是一个整体统一考虑，将安全的五大要素落实在信息化系统的每一个环节之上，从而形成对企业信息资源的全面保护。依据对现有企业安全架构的分析，企业应当在其安全架构中具备以下主要元素：

### 1）统一身份管理系统

统一的身份管理系统不仅仅需要对人进行管理，也要对相应的各种设备的身份进行管理，如自动柜员机、路由器和主机等等。另外，对企业之外的相关人员和设备也要进行管理，如某个 IP 地址所代表的设备等。身份的管理也包含了“黑名单”的管理，如垃圾邮件服务器等。

### 2）统一的认证机制和认证系统

认证系统负责对所有来访对象进行认证以确认来访者的合法身份。一旦来访者的身份获得认证之后，来访者取得合法的身份证并获得对资源访问的通行证。

### 3）统一的授权管理机制和系统

统一的授权管理机制和系统也是非常重要的。而且，认证机制和授权机制之间的匹配问题也是必须要考虑的，例如，是按组织机构还是按照角色进行授权就决定了“身份证”或“通行证”所必须提供的不同身份信息。

### 4）统一的信息保密技术和完整性保护技术

统一的信息保密技术和完整性保护技术也是在安全架构体系下必须考虑的问题。PKI技术的广泛使用已经为信息保密技术和完整性保护提供了标准化的技术。另外，针对安全问题的日志和审计系统也是非常重要的。

有了统一的身份管理、认证管理、授权管理，以及统一的信息保密技术和完整性保护技术，信息化的安全架构雏形就基本形成。另一个问题就是怎样与各个具体的资源管理和使用系统相结合，从而形成完整严密的信息安全体系。

企业的安全架构就是要制定出这些统一的安全机制和系统体系，同时考虑在信息化的各个环节的具体实施方法。安全架构的形成也是制定企业安全标准体系的一个不可缺少的途径。在安全架构之下，结合国家和国际的安全标准建立起一套完整的企业安全规范。

报告认为，在 08 年，企业信息安全架构发展的趋势为实现以上五点的统一、集成的企业安全架构，满足企业各个层面上的信息安全需求。

## 2、企业信息安全解决方案实施发展趋势分析

报告认为在 08 年，企业在信息安全实施上将增强反病毒、反恶意软件和反间谍软件的能力。来自这三种恶意程序的威胁呈不断增强的趋势，因此用户希望在实施全面集成的安全解决方案时，同时加强解决方案在病毒防护、恶意软件防护和间谍软件防护上的能力。

任何安全过程都是一个不断重复改进的循环过程，它主要包含风险管理、安全策略、方案设计、安全要素实施。依据目前各大安全产品厂商所提倡的信息安全解决方案实施发展策略，报告预计按照以下流程实施企业信息安全解决方案的流程将会在广大企业中得到广泛应用：

### 1）风险评估管理

对企业网络中的资产、威胁、漏洞等内容进行评估，获取安全风险的客观数据；

### 2）安全策略

指导企业进行安全行为的规范，明确信息安全的尺度；

### 3）方案设计

参照风险评估结果，依据安全策略及网络实际的业务状况，进行安全方案设计；

### 4）安全要素实施

包括方案设计中的安全产品及安全服务各项要素的有效执行；

### 5）安全管理与维护

按照安全策略以及安全方案进行日常的安全管理与维护，包括变更管理、事件管理、风险管理和配置管理；

### 6）安全意识培养

企业在实施安全解决方案的时，其中的一个重点将是帮助企业培训员工树立必要的安全观念。

## 3、企业信息安全投资趋势分析

### 1）基础安全产品投入稳步提升

对于仍然处于企业信息化进程当中的企业而言，有基础安全产品的投入将使得在这一领域的呈现稳步增长的趋势，报告认为 08 年企业尤其是中小企业将会增强在基础安全产品上的投入。与已经拥有较为完善的 IT 基础架构的企业不同，这些企业在实施企业信息化之处，即可以采用现有的、代表了企业安全架构发展方向的统一安全解决方案。

采用新的集成解决方案的 IT 投入将能够在今后相当长的时期内，仍然保持较高的可重用性和高利用率。

### 2）安全产品与应用软件关联性投资增加

为使安全产品能够更好地与企业现有 IT 资产紧密耦合，企业将加大安全产品与现有 IT 应用软件的关联性上的投资。

同时，对于已经有一定 IT 基础架构的企业而言，在实现安全产品与应用软件关联性的过程中，还将同时投资完成企业的基础架构优化和集成，以实现更方便地把新的 IT 应用集成到企业整体的 IT 环境中来，并为企业 IT 自然下一步重用和扩展打下基础。

### 3）企业将加大员工安全意识的培训投入

来自企业内部的威胁主要来自由于员工不当操作而造成的威胁，因此大多企业安全解决方案用户将在 08 年加大员工安全意识的培训投入，以其提升员工整体的安全操作和防护意识，降低来自企业内部的安全风险。从而以提供人的能动性而提高整体的生产能力。

# 四、企业信息安全解决方案实施建议

## 1、企业信息安全解决方案应达到的目标

企业的安全解决方案的最终目的应当是为企业业务的开展和实施提供技术支持，因此应用和实施安全解决方案应当达到以下目标：

### 1）高生产力

高效的安全解决方案不应以牺牲生产力为代价，企业 IT 经理们在决定实施安全解决方案之前，首先应对企业的实际业务需求做出详细的评估。安全解决方案实施的目标是能够提升企业的生产能力，为企业创造更高的效益。

企业采用的安全解决方案应当具备自动处理重复性任务的功能，通过自动执行重复性任务和嵌入到安全解决方案当中的知识捕获来增强企业的生产力，让企业能够在效益最大化的同时，维持最高水平的生产力。

企业可自动化处理的任务可以分为以下几类：

- **自动威胁响应：**在处理安全威胁的动态过程中，安全解决方案应当能够实现对安全威胁发现、分析、相应、信息再获取的四个环节实现全自动的监控与响应；
- **自动知识获取：**解决方案应当能够实现自动地对整个企业 IT 环境的威胁发现、分析、响应、信息再获取当中的信息进行捕获，从而自动地提升企业整体的安全响应水平。
- **自动软件分发：**对于已知安全威胁的安全补丁、防护程序更新的软件的分发，应当实现自动地软件分发，所有的客户端程序都能够自动地通过统一的控制中心进行分发。
- **其他的自动化过程：**除上述三个重要的方面以外，企业安全解决方案还应当能够实现流程自动化、威胁信息通知自动化等自动化过程，从而确保企业能够在较高的生产力下进行运作。

### 2）高度简化

在确保高生产力的目标实现的前提下，企业的安全解决方案应实现尽可能的简化，对于安全架构人员和安全实施人员而言，将减少很多后续的管理和维护工作，对于企业终端用户而言，不要花费太长时间的培训，用户即能够应用、升级、维护现有的安全防护。

企业采用的安全解决方案应当能够简化企业工作环境的部署、配置、管理和安全特性，提供至关重要的能见度，让企业 IT 管理人员能够随时随地做出必要的反应。

### 3）高度整合

在实现了企业现有的 IT 业务目标，确保企业高度生产能力以后，从整个企业 IT 管理的大局出发，企业采用的安全解决方案应当能够具备高度的整合性和扩展性。

企业采用的安全解决方案及其应用能够与管理基础设施实现无缝整合，进而提高企业系统的整体有效性和响应度，帮助企业实现投资价值的最大化。

## 2、优化基础架构

经过数年的投资，IT 经理们要面对大量要管理的 IT 基础设施，如何优化这些基础设施之间的关系，提升基础设施的功效能，为企业创造更多的收益，是 IT 经理们必须要面对的现状。企业应当构架提供自我管理的动态系统，运用信息技术来收集和利用知识以设计可管理性更高的系统，实现连续操作的自动化，最终实现降低成本。

在优化 IT 基础架构过程中，采取的解决方案应当具备以下特点：

### 1）知识驱动

通过收集和汇总与基础结构、策略、流程和最佳操作有关的知识，基础架构优化解决方案应该能够可以帮助企业主动管理 IT 环境，帮助 IT 提供商业所需的服务级别。

基础架构解决方案应当具备知识捕获的功能，捕获的信息可以用于设计可管理程度更高的应用系统，实现企业 IT 系统升级和优化的自动化，使这一持续的过程能够通过自动化的方式来实习和提高。

### 2）灵活性

基础架构优化解决方案应当能够提供灵活的 IT 管理，能够帮助用户分析、了解瞬息万变的业务需求，从而使 IT 进行有效地调整，满足不断发展的业务需求。

在应对新的业务需求时，IT 解决方案能够快速地针对新的业务需求做出调整，快速开发或引入新的功能，满足当前或短时期可能变化的新的需求。

### 3）可扩展性

基础架构优化解决方案应当是一个可扩展的解决方案套件，同时提供跨产品和技术的集成，可以将管理功能扩展到整个企业范围，使不同类型的环境能够更出色地协同工作。

在公司可能出现的并购、合并等案例中，基于相似 IT 基础架构的两个异构 IT 环境能够快速地整合为一个整体，引入和扩展新的 IT 应用将成为快捷简单的事情，使 IT 管理人员和实施人员在不断变化的业务需求带来的 IT 需求面前能够应对自如。

通过捕捉并汇总有关基础架构、策略、程序、以及最佳实践的知识，IT 基础架构解决方案应当能够帮助员工构建易于管理的系统并进行自动化操作，从而降低成本、提高应用系统的可用性、并改进所提供的服务。通过对操作系统、应用系统、合成服务和工作流等实现自内而外的依赖性评估和商业过程性能的优化。这样的 IT 基础架构解决方案将能够实现缩

小开发、操作和 IT 之间的差距，同时也应该提供针对物理和虚拟环境而实施的广泛管理，从而提高效率并增强控制。

## 3、强化 IT 环境防护

企业在进行 IT 管理的同时，更应防范来自各方的潜在威胁，这对 IT 管理人员提出了更高的要求。企业选用的安全解决方案，应当能够帮助企业实现保护企业敏感信息、控制对企业内部 IT 环境的访问等功能。

分类而言，对于企业中大量存在的应用程序服务器、消息和协作服务器、客户端等设备，IT 安全解决方案应当能够提供高级的安全和管理。

对于消息和协作服务器而言，安全解决方案应当能够对在企业邮箱、文档库和团队网站中传输及存储的宝贵数据提供高级的保护，它们有助于优化效率和性能，并容易部署和管理。

对于应用程序服务器而言，业界领先的安全产品是基于多重扫描引擎的服务器防护产品，与单一引擎解决方案相比，它能够提供更好的保护、更快速的新威胁检测、减少威胁的暴露，并减少单点故障的可能性,从而帮助保护客户的各种服务器免受病毒、蠕虫和垃圾邮件的侵扰。还应该具备防备未知文件和不良内容等功能，切实的 IT 安全保护将为企业 IT 环境带来更多保障。

对于客户端的安全而言，安全解决方案应当能够实现对商务桌面电脑，笔记本电脑和服务器操作系统提供统一的反病毒和反间谍软件保护，使之能够被更容易地管理和控制。

另外对于处于企业内部网络和外部网络“军事解禁”的企业网络边缘地带，应该采取专门的防护策略，实现保护 IT 环境不受基于互联网的威胁，并向用户提供迅速而安全的应用和数据远程接入，应当实现智能接入网关 SSL VPN 和端点安全特性管理解决方案，为企业分支结构和在外的销售人员等在总部之外的人员使用的设备，实现接入控制、授权和内容检查等功能。

在强化 IT 环境防护上，应当具备以下特点：

### 1）优化的性能

在采用多引擎扫描安全软件的基础上，企业还应当选择强大的多引擎管理软件，以用于自动的引擎更新和使用、多线程和内存扫描，能够进行更快地对引擎扫描的结果进行处理；同时应该能够平衡被防护对象的性能和安全需求水平。

把以上特性结合在一起，将有助于保护消息和协作系统，同时保持企业 IT 设施的正常工作时间，并优化其性能。

### 2）简化的管理

安全解决方案不应当由于功能性的提高而增加其复杂性，应当能够实现自动的引擎升级、扫描作业和报告等特性，从而使得管理员能够在所有被防护对象上轻松地管理和部署防护服务。简易的管理，可以通过中央管理来管理一台或更多计算机上的所有保护代理设置，并且能通过实用、有主次的安全报告和摘要仪表盘实现对系统运行状态的监控，从而能够拥有对恶意软件威胁的可见性和控制，从而更加高效地保护企业。

## 3）从源头保证安全

企业采用的安全解决方案应当具备全面的防护能力，最佳的解决方案是采用整合了来自许多行业领先安全公司的多个扫描引擎的安全应用程序。多引擎在一个解决方案中协同工作，与单一引擎解决方案相比，能够提供更好的保护、更快速的新威胁检测、减少威胁的暴露，并减少单点故障的可能性。这样的解决方案已经成为众多企业 IT 经理们优先考虑的安全解决方案。

网络是由包括个人计算机、台式机、工作站、服务器、网络设备等各种各样的端点组成的。报告显示，对企业网络构成的为首四大威胁全部都是源自终端。除了上面提到的病毒外，还有笔记本用户引起的交叉感染，内部终端的未授权访问，内部终端滥用网络。

根据国际计算机安全协会(ICSA Lab)的病毒调研报告，有 30%的终端不符合企业的安全要求。在蠕虫和病毒加速侵略我们的网络时，网络管理员们却发现自己迷失在终端管理的汪洋之中，疲于应对各种挑战。

各种端点是信息安全最核心的地方，如果从源头入手，把安全做进端点，就可以通过确保网络中每一个“端点”安全措施的完整，来保护整个网络的安全和 Web 应用的正常。在网络节点接入安全网络时，需要对接入的系统安全状况及系统用户的身份进行充分的分析、评估、认证，以此确认该系统是否符合网络的内部安全策略，是否达标，最后再决定是否需要给予该网络节点系统的接入权限，还是拒绝接入或是安全升级后再接入。

当侦测/预防系统检测到网络系统中存在异常情况（如病毒、蠕虫或木马程序等）时，就会将相关信息报告到策略控制系统，再由策略控制系统自动发出控制指令，通过准入安全设备将异常端点设备隔离，同时报告给网络管理员作进一步处理。系统就可以在短时间内控制发作范围，免去了因为人工操作时间较长，造成病毒或木马已经在网络内蔓延，难以控制的局面。通过准入设备、侦测/预防系统和策略控制系统的联动，将整个网络打造成预防、及时处理和策略控制的全面安全系统，如同可信计算一样，确保了所有接入到网络上的端点是可信的。这样网络就不会被滥用，有效降低了潜在的安全风险、降低了网络系统安全危机发生的频率、缩小了发生的范围、提高了处理的效率，降低了企业损失和成本。

# 总　结：

报告立足当前中国企业面临的整体安全环境，以最近两年的安全市场分析数据为依据，评估和预测 08 年安全领域将出现的整体趋势。致力于为企业 IT 经理和安全管理人员提供详尽的参考数据和安全解决方案实施建议。报告建议企业在实施任何一项 IT 解决方案之前都应该对企业的实际业务需求和投资回报进行详细的分析和评估，从而确保企业能够从 IT 投资当中获取最大的收益。

面对这些问题，企业可以通过中央管理方式以统一的处理为核心，统一防范现有和新出现的恶意软件，这样可以节省时间，降低复杂性。同时，企业通过可以监控整个企业中的关键威胁和潜在漏洞的工具，在应用系统里全方位的进行安全分析，从而拥有对恶意软件威胁的可见性和控制，并通过分析报告检查实时数据，查看新的趋势。此外，通过安装状态的仪表盘快照可以了解需要采取行动的位置；状态评估扫描可以确定哪些计算机需要修补程序，或配置不安全；安全警报可以在您环境中出现威胁时通知您。多引擎杀毒则可以避免因为单一杀毒软件的漏报导致内部网络的全线崩溃。

# 附录 A：术语及缩写

CA：Certification Authority，数字签证机构

PKI：Public key infrastructure，公钥基础架构

IDS：Intrusion Detection System，入侵检测系统

SM：Security Management，安全管理

EM：Enterprise Management，企业管理

CSPM：Centralized Security Policy Management，集中式安全策略管理

RTSA：Real-Time Security Awareness，实时安全监视

CM：Contain Mechanism，安全联动机制

CPM：Configuration and Patching Management，配置与补丁管理

PMAE：Privilege Management across the Enterprise，统一的权限管理

DM：Device Management，设备管理

ROI：Return Of Investment，投资回报

NPV：Net Present Value，净现值

IPS：Intrusion Prevention System，入侵防御系统

SSL：Secure Sockets Layer，安全套接层

VPN：Virtual Private Network，虚拟专用网络

IAM：Identity Access Management，认证访问管理

ES：Endpoint Security，终端安全

IGS：Internet Gateway Security，Internet 网关安全

SMB：Small and Midsize Business，中小企业业务

NAC：Network Access Control，网络访问控制

# 附录 B：参考资料

[1] Enterprise Network Security Equipment，Gartner

[2] Fishing Attacks Escalated in 2007，Gartner

[3] Biggest Information Security Mistakes that Organizations Make and How to Avoid Making Them，Security Information

[4] CSI Survey 2007-The 12th Annual Computer Crime and Security Survey, CSI/FBI

[5] End Point Security 2007，McAfee

[6] Identity Management Market 2005-2009，Radicati

[7] BSA-ISSA Information Security Study-Online Survey of ISSA Members，ISSA

[8] Top Information Security Risks for 2008，CISSPforum

[9] Market Trends: Security Markets，EMEA，2006-2011，Gartner

[10] Worldwide Security Software Revenue 2007，Gartner

[11] 中国 IT 安全市场分析与预测 2007-2011（1H07），IDC