

中小型企业用户网络安全解决方案



目录

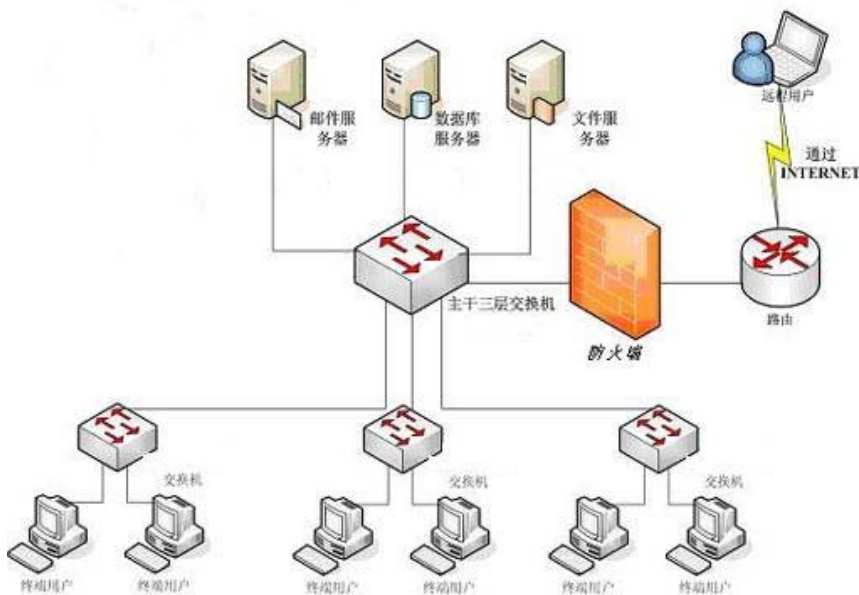
1. 中小型企业网络用户的网络环境	3
2. 中小型企业网络面临的安全风险问题	4
3. 网络安全问题的根源	6
4. 中小型企业安全解决方案	6
4. 1 解决方案的目标和原则	6
4. 2 内网防护产品	7
4. 3 网关防毒产品	8
4. 4 安全管理是治根之本	10
5. 服务体系	10

1. 中小型企业网络用户的网络环境

中小型企业防病毒系统应该具有系统性与主动性的特点，能够实现全方位多级防护，其中，与大型企业一样，中小企业同样需要网关防病毒。因为随着病毒技术的发展，病毒的入口点越来越多。即使网络上只联少数机器的中小型企业也需要考虑在每一种需要防护的平台部署防病毒软件，绝不能因为企业的规模大小，就单纯地认为他们的防病毒系统可以简化，麻雀虽小也是五脏俱全。

200-300 点的中小型企业防病毒体系应该包括：客户端，不管客户端使用什么操作系统，都必须具有相应的防病毒软件进行安装防范；邮件服务器，电子邮件目前已经成为病毒传播的重要途径，一个好的邮件或群件病毒防范系统可以很好地和服务器的邮件传输机制结合在一起，完成对服务器以及邮件正文的病毒清除工作。目前邮件病毒的传输方式已经从以前的单纯附件携带方式扩展为内容携带方式；其他服务器，网络中除了邮件服务器外，还存在大量的其他服务器如文件服务器、应用服务器等，这些服务器也需要安装相应的防病毒软件；网关，网关是隔离内部网络和外部网络的设备如防火墙、代理服务器等，在网关级别进行病毒防范可以起到对外部网络中病毒进行隔离的作用。

网络环境拓扑图如下：



由于资金、技术等方面的原因，中小型企业的安全问题一直隐患重重。据了解，许多企业没有设置专门的网络管理员，一般采用兼职管理方式，这使中小企业的网络管理在安全性方面存在严重漏洞，与大型企业、行业用户相比，它们更容易受到网络病毒的危害，损失同样严重。另一方面，由于网络维护、运行、升级等事务性工作繁重而且成本较高，这也使

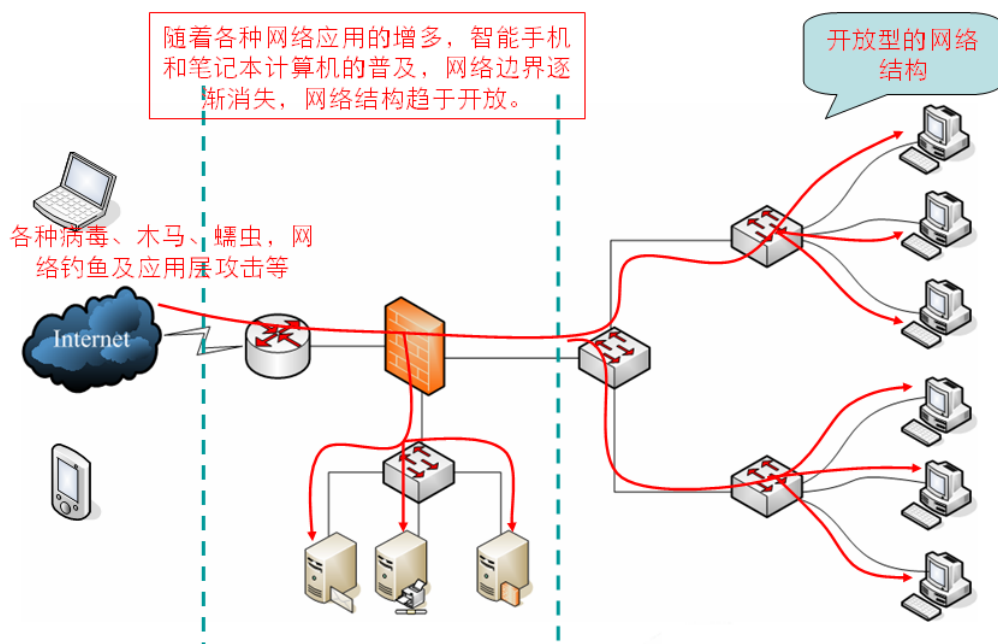
得善于精打细算的企业在防范病毒问题上进退两难。

有些中小型企业往往对于病毒心存侥幸。殊不知，病毒威胁无处不在，从近来病毒发作的情况来看，病毒的击目标没有特定性，而且越来越隐蔽，如不提前防范，一旦被袭，网络阻塞、系统瘫痪、信息传输中断、数据丢失等等，无疑将给企业业务带来巨大的经济损失。无论是我们熟知的 CIH、I love You 和 Melissa，还是 SriCam、CodeRed、Nimda 和 Goner 等，可能正在从桌面、服务器、邮件服务器、Internet 网关等各个点侵入到企业网络。如同大型企业一样，中小型企业防病毒体系的建立呼之欲出。

2. 中小型企业网络面临的安全风险问题

在当前全球化的商业竞争环境下，中小型企业要在拓展业务和改善客户满意度的同时严格地控制运营成本。幸运的是，互联网和网络应用程序使几乎所有的企业都处于同一起跑线上。中小型企业可以借助互联网来开拓市场，改善与客户和合作商的沟通效率。然而，迅速快捷的电子商务也是一把双刃剑，它可能为企业带来代价高昂的安全问题。对于企业来说，拥有一个可靠、安全和时刻可用的网络是非常重要的。

研究表明，安全问题是中小型企业目前面临的巨大挑战。来自企业内部和外部的动态变化的安全威胁随时会给企业运营带来巨大的灾难，并最终影响企业的盈利能力和客户满意度。



风险一：病毒长驱直入，内网防毒压力大

在网络病毒盛行的今天，病毒最主要的传播途径是通过互联网。如果在网络入口的地方缺少相应的保护，那么病毒就会长驱直入到内部网络，一旦病毒达到内网，把防毒的压力全部放在桌面端，经过分析，大部分病毒事件都和用户上网行为相关，如果在网关处增加一道屏障，内部计算机感染病毒的可能性就会大大的下降。

风险二：缺乏系统的风险控制方法和策略，安全策略无法落实，隐患重重

“三分技术，七分管理”是众所周知的基本原理，想要有效的控制风险，就必须有一套行之有效的安全策略，并且能够将安全策略加以落实。企业虽然已经制定了《网络与计算机使用规范》，如：要求所有的员工必须安装系统与应用补丁，必须安装防毒软件，防毒软件必须做到及时更新。但实际上，企业很少有员工真正遵循该规范要求，很多员工的PC都没有更新最新的系统补丁，这成为病毒很容易侵入到公司网络的重要原因。

风险三：桌面防毒各自为战，难以抵御网络病毒

桌面防毒是查杀病毒的最后一道防线，部署率和更新率是防毒体系是否完整的重要依据，而获得更高的部署率和更新率的有效手段是运用中央控管功能，由管理员统一的分发防毒软件，统一的部署更新组件，及时地掌握每个客户端的防毒状况，从而做出有效的响应和应对措施。公司现有的桌面防毒软件在统一管理特性上严重不足，容易成为防护体系中的短板。

风险四：管理员四处救火，缺少主动防御措施

企业几乎每天都有计算机中病毒，几乎每隔几天都有人要重装系统。企业仅有的专业管理人员成了公司最忙碌的人，四处救火。当一个新病毒爆发的时候，管理员往往只能被动的等待病毒特征码的发布，在获得最新的病毒码之前，几乎只能坐以待毙。企业缺乏面对新病毒爆发时候的响应措施和流程，所以每次病毒爆发对公司信息系统的影响都很大。

风险五：员工安全意识淡薄，上网行为混乱

在整个信息系统存在的薄弱点中，人恐怕是最至关重要的。因为员工安全意识的淡薄，原本可以避免的安全事件会酿成恶果。内部员工可以随意的在网络上下载文件，随意的访问形形色色的网站，往往把间谍软件和病毒引入到公司网络。

通过以上的风险分析，我们评估中小型企业网络安全可能面临的威胁：

1) 抢占系统资源，影响计算机运行速度。大多数病毒在动态下都是常驻内存的，这就必然抢占一部分系统资源。病毒进驻内存后不但干扰系统运行，还影响计算机速度。

2) 对计算机数据信息造成破坏作用。大部分病毒在激发的时候直接破坏计算机的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无

意义的“垃圾”数据改写文件、破坏 CMOS 设置等。

3) 黑客通过系统漏洞进入用户的系统并隐藏，然后向盗取用户的信息，对用户的资源财产具体相当大的破坏性。

4) 可能终端都各自部署了自己的杀毒软件，但是由于内网病毒的交叉感染，导致病毒不能够被彻底的清除，整个网络受到严重的影响。

3. 网络安全问题的根源

目前，中小型企业用户占我国企业主体比重非常大，但由于分布散，购买力等原因，中小型企业的安全问题似乎一直没有得到安全厂商的足够重视。市场上的安全产品五花八门种类繁多，防病毒、防火墙、信息加密、入侵检测、安全认证、核心防护无不囊括其中，但从其应用范围来看，这些方案大多数面向银行、证券、电信、政府等行业用户和大型企业用户，针对中小型企业的安全解决方案寥寥无几，产品仅仅是简单的客户端加服务器，不能完全解决中小型企业用户所遭受的安全威胁。目前，国内厂商推出了网络版病毒软件，但由于功能的单一，并不能为中小型企业提供完善的防护。

其实，安全的漏洞往往存在于系统中最薄弱的环节，邮件系统、网关无一不直接威胁着企业网络的正常运行；中小型企业需要防止网络系统遭到非法入侵、未经授权的存取或破坏可能造成的数据丢失、系统崩溃等问题，而这些都不是单一的防病毒软件外加服务器就能够解决的。因此无论是网络安全的现状，还是中小型企业自身都向广大安全厂商提出了更高的要求。

构筑具有必要的信息安全防护体系，建立一套有效的网络安全机制显得尤其重要，而建立中型网络安全体系，主要依赖三个方面：一是威严的法律；二是先进的技术；三是严格的管理。

4. 中小型企业安全解决方案

根据中小型企业的网络安全体系的防毒现状和需求提出的针对性解决方案。该方案为企业提供全方位的防护，可以应对病毒、间谍软件、木马、钓鱼程序、垃圾邮件、Web 安全、内容过滤、安全管理等安全问题，提供了从桌面端、服务器、网关防护的多层次防护体系，可供选择的专业的安全服务加深了防护深度。

4.1 解决方案的目标和原则

解决方案的具体目标:

- 1) 有效的控制网络恶意程序等安全威胁
- 2) 有效的控制垃圾邮件和病毒邮件扩散
- 3) 有效的加强安全策略管理和执行力度
- 4) 有效的对员工上网行为加强控制
- 5) 确保病毒事件有及时有效的相应机制和防护措施
- 6) 降低网络管理人员的工作量

解决方案的构建原则:

- 1) 经济实用性原则

企业对安全防护系统的投入将遵循经济实用性原则，在选择方案时，性能价格比是最重要的衡量标准之一。

- 2) 简单易用性原则

公司对 IT 人员的投入有限，IT 专业管理人员同时需要负责网络、系统、应用系统的维护，所以平台的易用性，操作的简便性，部署的方便性就显得尤其重要。

- 3) 先进性原则

网络安全解决方案的选择应该同时考虑到技术上的先进性，IT 技术日新月异，威胁种类变化多端，只有掌握了最新防毒技术，有着深厚技术背景的供应商才可以提供企业及时地防护。所以选择技术方案时，厂商的技术实力、技术支持力度、品牌也是关键。

4.2 内网防护产品

据统计，网络是目前绝大多数病毒传播的主要途径。对于一个网络系统而言，针对病毒的入侵渠道和病毒集散地进行防护是最有效的防治策略。因此，对于每一个病毒可能的入口，部署相应的反病毒软件，从而进行实时检测，是构建一个完整有效内网防护体系的关键。而内网防护体系的建立需要达到如下的功能效果。

- 1) 简易的安装和配置操作

对于现今的企业来说，Internet 访问的稳定性、安全性十分重要。防毒产品的安装和设置应尽量简易，充分考虑大学校园网系统数据、文件的安全可靠性，所选产品与现系统具

有良好的一致性和兼容性，以及最低的系统资源占用，保证不对现有系统运行产生不良影响。

2) 可管理性

企业日益重视其 IT 环境的总体拥有成本。在有限的人力资源情况下，IT 管理员的工作是非常复杂和繁忙的，要管理好防病毒系统的安装、升级、配置和工作报告是一个非常繁琐的事，因此产品本身应带有集成的、易用的管理工具，管理员可以从一个集中管理控制台对整个防毒系统进行监控管理和维护，做到客户端的零操作。

3) 软件的可升级性

可升级能力是衡量防病毒系统是否具有生命力的重要指标。防毒软件的特点是随着各类新病毒的出现而必须尽快进行更新和升级，其中包括病毒定义、产品组件的更新。

4) 强大的病毒清除能力

如果选用的防病毒软件病毒清除能力较弱，在病毒爆发的情况下，管理员会为了彻底清除网络中的病毒而疲于奔命，即使采用病毒专用清除工具，在城域网或广域网中也存在工具的分发和终端用户是否使用的问题，这样在较长时间内整个城域网或广域网中病毒会一直存在。采用世界最先进的清除病毒能力较强的防毒产品，可确保大学校园网计算机网络系统具有最佳的病毒、黑客软件防护能力。同时也降低了管理人员的工作量和防病毒产品的维护成本。

5) 优秀的产品性能

选用产品应具备对多种文件格式、多层压缩文件的病毒检测，对包括各种宏病毒、变体病毒和黑客程序等已知病毒具有最佳的病毒检测率，对未知病毒亦有良好的检测能力。在提高病毒检测力的同时，对检测出的病毒也有很高的清除能力，依靠程序本身就可彻底清除感染文件的病毒，减轻管理人员对中毒事件的介入，把更多的精力放在构建完整的病毒防护体系和管理工作上。

6) 新病毒的快速响应

在全球范围内每周产生大约 300 只新病毒的情况下，每周的病毒库更新使用户在病毒出现后和下次更新前，会存在感染病毒而防病毒软件根本无法识别的风险。而每小时一次病毒数据库的更新，紧急情况下 30 分钟的全球用户更新，确保在任何新病毒出现的情况下通过快速高效的防病毒更新机制，使所有用户得到最大程度的防病毒保护。

因此对于整个内网而言，需要采取综合的防护措施，构筑全方位的安全保护系统，才能得到真正有效的系统安全。

4.3 网关防毒产品

防毒墙是基于协议栈工作，或称工作在 OSI 的第七层；而防火墙是基于 IP 栈工作，即 OSI 的第三层。因此决定了防火墙必须以管理所有的 TCP/IP 通讯为己任，而防毒墙却是以重点加强某几种常用通讯的安全性为目的。因此，对于用户而言，两种产品并不存在着互相取代的问题，防毒墙是对防火墙的重要补充。在实际应用中，防毒墙的作用在于对所监控的协议通讯中所带文件中是否含有特定的病毒特征。

随着利用网络传播的恶意程序大量出现，局域网各终端节点的防护压力越来越大，其中突出表现在以下方面：1) 下载文件造成病毒侵入——由于许多个人网站上的下载文件实际为伪装的木马程序，员工在访问时常常在不知不觉中将病毒下载并激活，造成终端节点频频病毒爆发；2) 网页内嵌恶意程序——当员工浏览内嵌有恶意程序的网站时，由于自身系统的安全漏洞，常常造成恶意程序自动执行，造成诸如强制修改 IE 设定、不断弹出窗口等后果，影响员工的正常工作；3) 恶意 URL 不能自动阻止——对于内嵌恶意程序的 URL 的访问，由于不能实施自动阻止策略，造成同一种恶意程序不断侵入企业网络；4) 非工作相关站点的访问——员工在工作时间访问与业务无关的站点，如游戏、娱乐等网站，造成员工生产力下降。

针对以上因素，为了实现网关防毒功能，在选择网关防毒产品时要实现如下功能：

- 1) 强劲杀毒引擎，深度威胁防御系统，面向安全特性的专用处理硬件和软件平台，为保护高速局域网和低速广域网连接提供所需性能。
- 2) 网络分区等高级安全特性允许管理员部署安全策略，将访客、无线网络以及地区服务器或数据库相隔离，以防止未经授权的接入并阻止任何可能发生的攻击。
- 3) 防毒新技术保持前沿最新状态，时刻保持病毒库更新的及时和高效，确保网络免遭蠕虫、间谍软件、特洛伊木马、恶意软件及其他新兴攻击的侵袭。
- 4) 具有全方位的安全服务——防火墙、VPN、入侵检测 (IPS)、防病毒、内容过滤等多种功能，很好的解决了在网络中遇到的各种问题。
- 5) 对通过邮件传播的病毒进行过滤。防毒墙能够有效的对 SMTP, POP3 协议进行检

测，能够对于通过电子邮件传播的病毒进行有效的防范。

通过部署网关级防毒产品，能够在网络入口处直接对恶意程序进行防护，有效阻止其长驱直入，对于 HTTP, FTP, POP3, SMTP 的防护，可以使终端在进行网页浏览，文件下载，收发邮件时更加得心应手，不再受到弹出窗口，病毒木马，垃圾邮件的困扰。

4.4 安全管理是治根之本

“三分技术，七分管理”是众所周知的基本原理，想要有效的控制风险，就必须有一套行之有效的安全管理策略，并且能够加以落实。外围防御战略的最显著特征之一就在于安全基础设施中每台设备会产生极大量的事件数据。在一个中小型企业中，一台设备每一天都会产生多达十亿字节的信息。同样，一个IDS检测器每一天也可产生500,000多条消息。这就表明了安全管理的一个首要问题：安全设备所产生的数据量实在太多，导致安全团队无法有效监控——更不要说关联了。

利用传统的安全分析方法，安全操作员可监控整个企业中的活动来揭示网络攻击或漏洞。他们必须以手工方式来处理每台安全设备中所包含的极大量信息才能创建关于正在发生事件的全面视图。以这种过时和无效的方法为基础建立法律分析系统的过程既耗费时间又代价高昂，而且还会占用本可用于其他更有价值的运营和/或安全活动的专家资源。此外，传统的安全数据分析方法需要若干天或若干周来执行。到分析结束时，网络也许已经遭到了若干次攻击，并可因数据盗窃、客户和合作伙伴失去服务或机构生产效率降低等而导致重大损失。

鉴于这一现实，以技术为基础的实时安全数据监控和关联系统也就应运而生即一款安全管理软件，它能够实现如下功能：

- 1) 实时收集安全设备系统信息，随时跟踪锁定目标
- 2) 提供互动的直观图形化显示，病毒系统故障和活动一目了然
- 3) 通过 Web portal 用户无论何时何地都可以进行了解安全情况
- 4) 关联所有病毒信息，安全报警更加精确
- 5) 提供快速响应机制

安全管理平台的系统可利用规范化、汇聚和关联等技术实时筛选和分析极大量的安全活动数据——对各类事件进行关联，标记并评估所有攻击、影响和漏洞的潜在严重性。可以帮助我们减轻监控安全基础设施所需要承担的手工工作量。通过实现自动化的智能化诊断、分析和响应模板，可由IT管理人员针对各种不同风险情况进行选择和定制。解决方案可极大加

快机构面对IT危机时的响应和恢复速度，同时还能有效地使人员编制保持较低水平，总拥有成本可以得到降低

5. 服务体系

浙江金财信息科技有限公司是一家专注于网络信息安全的专业技术企业，公司聚集了一支在网络信息安全领域的有着丰富经验的专业技术团队，针对病毒、蠕虫、木马、垃圾邮件、黑客、非法入侵、间谍软件、流氓软件、不良网页、不良网络行为、信息泄漏、数据丢失、毁损等各类网络信息安全隐患，为客户提供技术咨询、完整的信息安全解决方案、国际顶级的软硬件工具，及时相应的专业技术支持。

公司作为国际顶级反病毒专业公司——卡巴斯基实验室的华东、华中技术服务中心及唯一总代，国际著名网络专业公司Novell的金牌代理，将卡巴斯基卓越的反病毒、反黑客、反垃圾邮件以及Novell网络资源管理、网络身份认证、linux的技术和服务推荐给广大用户。同时，公司还是网康互联网控制管理产品及服务和硕琦邮件服务器、反垃圾邮件网关的核心代理。此外公司还与国际、国内网络信息安全的著名厂商有着密切的合作和交流。

公司拥有广泛的客户群，涵盖各级政府、电信、银行、保险、证券、大中小学、大中型生产企业、大型商业连锁、各类设计院、各类网站等各行各业的网络用户。

公司与其战略合作伙伴——北京华商达、上海玖道、上海威迪、上海道弘、杭州宏运——一起充分合作，在遍及全国的500多家渠道、技术合作伙伴的大力支持下，凭借专业的技术团队、丰富的技术经验以及遍布全国的服务网点，协助用户在虚实相间、危机四伏的网络世界中享受一片宁静、高效的网络天地。

服务内容：

- 1) 提供完整的网络安全整体解决方案。
- 2) 提供日常工作日的电话，邮件，通讯远程协助等服务。
- 3) 遇到重大病毒事件提供免费的上门服务，给用户完善处理问题。
- 4) 提供及时的产品试用与培训服务。

卡斯基华东总代

浙江金财信息科技有限公司

杭州文三路555号浙江中小企业大厦1918室

Tel: 0571-28837715

Fax: 0571-88211520