 1.Cisco公司的NetRanger 1996年3月，WheelGroup基于多年的业界经验推出了NetRanger。产品分为两部分：监测网络包和发告警的传感器(9000美元)，以及接收并分析告警和启动对策的控制器(1万美元)。 另外，至少还需要一台奔腾PC来跑传感器程序以及一台Sun SparcStation通过OpenView或NetView来跑控制器程序。两者都运行Sun的Solaris。在软硬件平台中，传感器上可能要花费1.3万美元，控制器上要花费2.5万美元。 NetRanger以其高性能而闻名，而且它还非常易于裁剪。控制器程序可以综合多站点的信息并监视散布在整个企业网上的攻击。NetRanger的最大名声在于其是针对企业而设计的。这种名声的标志之一是其分销渠道，EDS、Perot Systems、IBM Global Services都是其分销商。 NetRanger在全球广域网上运行很成功。例如，它有一个路径备份(Path-doubling)功能。如果一条路径断掉了，信息可以从备份路径上传过来。它甚至能做到从一个点上监测全网或把监测权转给第三方。 NetRanger的另一个强项是其在检测问题时不仅观察单个包的内容，而且还看上下文，即从多个包中得到线索。这是很重要的一点，因为入侵者可能以字符模式存取一个端口，然后在每个包中只放一个字符。如果一个监测器只观察单个包，它就永远不会发现完整的信息。 按照GartnerGroup公司的研究专家Jude OReilley的说法，NetRanger是目前市场上基于网络的入侵检测软件中经受实践考验最多的产品之一。 但是，对于某

些用户来讲，NetRanger的强项也可能正好是其不足。它被设计为集成在OpenView或NetView下，在网络运行中心(NOC)使用，其配置需要对Unix有详细的了解。NetRanger相对较昂贵，这对于一般的局域网来讲未必很适合。 2.Network Associates公司的CyberCop Network Associates 公司是1977年由以做Sniffer类探测器闻名的Network General公司与以做反病毒产品为专业的 McAfee Associates公司合并而成的。NetWork Associates从Cisco那里取得授权，将NetRanger的引擎和攻击模式数据库用在CyberCop中。 CyberCop基本上可以认为是NetRanger的局域网管理员版。这些局域网管理员正是NetWork Associates的主要客户群。其软件价格比NetRanger还贵:传感器为9000美元，服务器上的控制器为15000美元。但其平台却可以是运行Solaris 2.5.1的Dell PC(通常CyberCop是预装在里面的)。跑传感器的平台一般要3000美元，控制器的平台要5000美元。 另外，CyberCop被设计成一个网络应用程序，一般在20分钟内就可以安装完毕。它预设了6种通常的配置模式:Windows NT和Unix的混合子网、Unix子网、NT子网、远程访问、前沿网(如Internet的接入系统)和骨干网。它没有Netware的配置。 前端设计成浏览器方式主要是考虑易于使用，发挥Network General在提炼包数据上的经验，用户使用时也易于查看和理解。像在Sniffer中一样，它在帮助文档里结合了专家知识。CyberCop还能生成可以被 Sniffer识别的踪迹文件。与NetRanger相比，CyberCop缺乏一些企业应用的特征，如路径备份功能等。 按照CyberCop产品经理Katherine Stolz的说法，Network Associates公司在安全领域将有一系列的举措和合作。"我们定位在大规模的安全上，我们将成为整体解

决方案的提供者。" 3.Internet Security System公司的RealSecure 按照GartnerGroup的OReilley的说法，RealSecure的优势在于其简洁性和低价格。与NetRanger和CyberCop类似，RealSecure在结构上也是两部分。引擎部分负责监测信息包并生成告警，控制台接收报警并作为配置及产生数据库报告的中心点。两部分都可以在NT、Solaris、SunOS和Linux上运行，并可以在混合的操作系统或匹配的操作系统环境下使用。它们都能在商用微机上运行。 对于一个小型的系统，将引擎和控制台放在同一台机器上运行是可以的，但这对于NetRanger或CyberCop却不行。RealSecure的引擎价值1万美元，控制台是免费的。一个引擎可以向多个控制台报告，一个控制台也可以管理多个引擎。 RealSecure可以对CheckPoint Software的FireWall-1重新进行配置。根据入侵检测技术经理Mark Wood的说法，ISS还计划使其能对Cisco的路由器进行重新配置，同时也正开发OpenView下的应用。 4.Intrusion Detection公司的Kane Security Monitor 基于主机的Kane Security Monitor(KSM) for NT是1997年9月推出的。它在结构上由三部分组成，即一个审计器、一个控制台和代理。代理用来浏览NT的日志并将统计结果送往审计器。系统安全员用控制台的GUI界面来接收告警、查看历史记录以及系统的实时行为。KSM对每个被保护的服务器报价1495美元(包括审计器和控制台)，在此基础上每个工作站代理报价295美元。 按照位于加州Playa Del Rey以安全技术见长的Miora Systems Consulting公司的资深咨询专家David Brussin的看法，KSM在TCP/IP监测方面特别强。但他也提到，Intrusion Detection的产品不是为较快的广域网设计的。 公司的奠基人兼总裁Robert Kane说

，Intrusion Detection在本季度将推出在OpenView下的应用，随后在年底将推出与Tivoli Management Environment(TME)的集成。将来，Intrusion Detection还计划支持Unix、微软的BackOffice和Novell的Netware。 5.Axent Technologies公司的OmniGuard/Intruder Alert 与KSM的审计器、控制台、代理所对应的OmniGuard/Intruder Alert(ITA)在结构上的三个组成部分为一个管理器(1995美元)、控制台(免费)和代理(每个服务器为995美元，每个工作站为95美元)。 ITA比Intrusion Detection的KSM提供了更广泛的平台支持。它的管理器和代理能在Windows NT、95、3.1和Netware 3.x、4.x上运行，所有的部分在多种Unix下都能运行，如Solaris、SunOS、IBM AIX、HP-UX以及DEC的Unix。 可以根据一些解决方案来剪裁ITA，这些解决方案可来自主流的操作系统、防火墙厂商、Web服务器厂商、数据库应用以及路由器制造商。Axent在2月份兼并了防火墙厂商Raptor，并将增强ITA，使其能对Raptor的防火墙进行重配置。 6.Computer Associates公司的SessionWall-3/eTrust Intrusion Detection SessionWall-3/eTrust Intrusion Detection可以通过降低对网络管理技能和时间的要求，在确保网络的连接性能的前提下，大大提高网络的安全性。SessionWall-3/eTrust Intrusion Detection可以完全自动地识别网络使用模式，特殊网络应用，并能够识别各种基于网络的各种入侵、攻击和滥用活动。另外，SessionWall-3/eTrust Intrusion Detection还可以将网络上发生的各种有关生产应用、网络安全和公司策略方面的众多疑点提取出来。 SessionWall-3/eTrust Intrusion Detection是作为一种独立或补充产品进行设计的，它的特点包括： 世界水平的攻击监测引擎

，可以实现对网络攻击的监测；丰富的URL控制表单，可以实现对200，000个以上分类站点的控制；世界水平对Java/ActiveX恶意小程序的监测引擎和病毒监测引擎；SessionWall-3/eTrust Intrusion Detection远程管理插件，用于没有安装SessionWall-3/eTrust Intrusion Detection的机器的SessionWall-3/eTrust Intrusion Detection记录文件的归档和查阅，以及SessionWall-3/eTrust Intrusion Detection报表的查阅。SessionWall-3/eTrust Intrusion Detection的网络安全保护SessionWall-3/eTrust Intrusion Detection屡获殊荣，是最全面的网络安全管理软件。 SessionWall-3/eTrust Intrusion Detection的特点包括： 提供从先进的网络统计到特定用户使用情况的统计的全面网络应用报表；网络安全功能包括内容扫描、入侵监测、阻塞、报警和记录。 Web和内部网络使用策略的监视和控制，对Web和公司内部网络访问策略实施监视和强制实施；公司保护（Company preservation），或称诉讼保护，即对电子邮件的内容进行监视，记录、查看和存档；SessionWall-3/eTrust Intrusion Detection还包括用于WEB访问的策略集（用于监视/阻塞/报警）和用于入侵监测的策略集（用于攻击监测、恶意小程序和恶意电子邮件）。这些策略集包含了SessionWall-3/eTrust Intrusion Detection对所有通信进行扫描的策略，这些策略不仅指定了扫描的模式、通信协议、寻址方式、网络域、URL以及扫描内容，还指定了相应的处理动作。一旦安装了SessionWall-3/eTrust Intrusion Detection，它将立即投入对入侵企图和可疑网络活动的监视，并对所有电子邮件、WEB浏览、新闻、Telnet和FTP活动进行记录。SessionWall-3/eTrust Intrusion Detection还可以很方便地追加新

规则，或利用菜单驱动选项对现有规则进行修改。
SessionWall-3/eTrust Intrusion Detection可以满足各种网络保护需求，它的主要应用对象包括审计人员、安全咨询人员、执法监督机构、金融机构、中小型商务机构、大型企业、ISP、教育机构和政府机构等。 SessionWall-3/eTrust Intrusion Detection的功能 SessionWall-3/eTrust Intrusion Detection是一种功能全面且使用方便的网络保护解决方案，它克服了网络保护中的主要业务障碍，其采用的主要手段包括： 最大程度地降低用户技能和资源需求； 提供一种经济的和可扩展的解决方案； 提供管理报表； 提供灵活易用的工具。 从操作的角度讲，SessionWall-3/eTrust Intrusion Detection去除了某些网络保护解决方案在安装和操作的麻烦。实际上
，SessionWall-3/eTrust Intrusion Detection可以提供许多人们所期望网络内在特性，而这些特性在过去是必需借助多种工具并通过复杂的分析之后才能够得到的。为了达到这一目的
，SessionWall-3/eTrust Intrusion Detection采用了如下措施： 即插即用安装（自动配置）； 易用的图形用户界面； 登录网络活动的在线查阅； 实时统计和图形显示； 全面的"追根溯源（drill down）"报表； 联机查询和定时报表； 易于更新的监视、阻塞和报警规则； 综合的响应和报警集合，包括实时干涉，预定义阻塞规则、第三方应用启动响应接口、以及不同的信息发送方式。 用于监视和阻塞的全面URL站点分类和控制列表。 支持WEB自速率系统（RSACi）。 先进的可疑小程序监测（例如，Java/ActiveX引擎）。 综合病毒扫描引擎和病毒库。 完整的格式化内容和附件浏览器。 电子文字模式内容的扫描和阻塞； 菜单驱动的自动地址解析。 特殊的保密特性

，可以对控制访问权限提供登录和管理的访问控制。
SessionWall-3/eTrust Intrusion Detection的特点
SessionWall-3/eTrust Intrusion Detection与大多数网络保护产品不同，后者是生硬地安插在网络通信路径中的，而前者则是完全透明的，它不需要对网络和地址做任何的变化，也不会给独立于平台的网络带来任何的传输延迟。
SessionWall-3/eTrust Intrusion Detection可全面满足你的需要！
SessionWall-3/eTrust Intrusion Detection代表了最新一代Internet和Intranet网络保护产品，它具备前所未有的访问控制水平、用户的透明度、性能、灵活性、适应性和易用性
。SessionWall-3/eTrust Intrusion Detection无需使用昂贵的UNIX主机，也避免了因非路由防火墙所造成的额外开销。另外，SessionWall-3/eTrust Intrusion Detection还包括一个会话视窗，可以用于网络入侵的监视、审计，并可以为电子通信的滥用现象提供充分的证据。 技术规范 操作系统：Windows 95（OSR 2）， Windows 98或Windows NT 4.0（SP3以上）以上版本； 系统平台：Intel Pentium 100MHz以上； 内存：64MB RAM 磁盘空间：200MB可用空间 网络接口：标准以太网/令牌环网/FDDI 软件介质：CD-ROM 7.Trusted Information System公司的Stalkers 由Haystack Labs于1993年推出的Stalker是一个基于主机的监测器，它能用于NT以及多种版本的Unix，包括Solaris、AIX、HP-UX和SCO的 UnixWare
。2.1版的管理器价格为9995美元，每个代理为695美元。
Haystack Labs在1996年6月推出了WebStalker Pro，其操作系统运行平台和Stalker是一样的，但其使用对象是Web服务器。它在Unix下的报价是4995美元，在NT下的报价是2995美元。Sun

的Netra Web服务器在销售时就带有一个WebStalker的专门版。IBM Global Services也销售WebStalker。 开发基于NT防火墙产品Gauntlet的Trusted Information System公司于1997年10月收购了Haystack。于1997年12月宣布了只在NT下运行且为微软的Proxy Server 2.0设计的监测器ProxyStalker。ProxyStalker计划于第一季度推出，其价格尚未宣布，但估计和Proxy Server应该是同等档次的产品，即少于1000美元。 所有三种Stalker产品都可以对防火墙产品Gauntlet重新配置，三种产品也都可以在发现入侵的同时消灭入侵。例如，WebStalker Pro可以终止一个登录或一个进程，它也可以重启一个Web服务器。Stalker家族也能与TME集成在一起。 