安全的

伊索寓言

China Network World

网络世界

网络安全专刊

安全的

伊索寓言

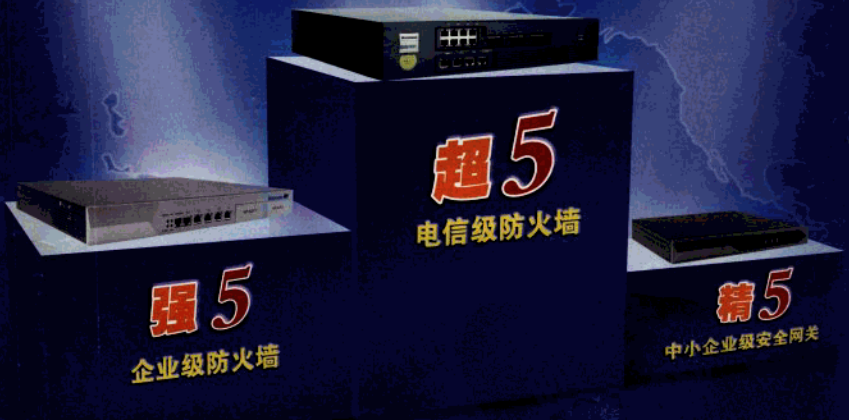
China Network World

网络世界

网络安全专刊


会议开始之际，蠕虫病毒开始攻击网络。
然而甚至在您的议程开始之前，入侵
的蠕虫早已被发现、隔离并完全清除！
趋势科技和思科系统——携手合作
想像一个您真正期待的网络安全解决方案：先进、安全、睿智，牢不可破……
从此您将再也不必担心企业内部的病毒爆发。
更多信息请访问：www.trendmicro.com/cisco
CISCO SYSTEMS
Technology
Developer
Partner
TREND
MICRO

随御而安，只要你想！



联想网御防火墙国内品牌用户市场份额持续领先 (IDC 2004 上半年度报告)

联想网御全线安全产品

超五系列千兆线速防火墙

- 网御Super V-7400
- 网御Super V-7308

强五系列防火墙

- 网御Power V-3000
- 网御Power V-400
- 网御Power V-300
- 网御Power V-200

精五系列安全网关

- 网御Smart V-100
- 网御Smart V-50
- 网御Smart V-25

VPN SJW44系列产品

- 网御VPN SJW44-400
- 网御VPN SJW44-300
- 网御VPN SJW44-C
- 网御VPN SJW44-SMC

IDS入侵检测系列产品

- 网御IDS N5000
- 网御IDS N3000
- 网御IDS N800
- 网御IDS N100

SIS-3000安全隔离与信息交换系统

- 网御SIS-3000

联想网御安全管理平台

lenovo 联想
只 要 你 想

联想（北京）有限公司　北京8688信箱
邮编：100085
售后服务热线：010－58863266
销 售 热 线：010－58861770
信息安全网站：www.infosec365.com.cn
E-mail支持：infosec@lenovo.com
联想网站：www.lenovo.com

前言

谁是金蛋上的那只鹅?

几乎在一夜之间，安全产业成了令人垂涎的“金蛋”。在利好报告不断的怂恿下，在一波波收购与兼并的热潮中，所有相关厂商都争先恐后，要成为坐在金蛋上的那只鹅。

然而，仅靠机运并不能催生一家伟大的企业，一个产业的成长与发展，也绝不可能在简单的争夺与占有之中完成。安全对于信息产业乃至整个社会的特殊意义，更决定了它的每一步前行，都需要我们三思而定。

细读伊索寓言中金蛋与鹅的故事，可以带给我们更多的启发：农夫养了一只吃玉米和清水，就能下出金蛋的鹅，然而每天得到一个金蛋，仍然让他无法满足。为了尽快地发财，农夫剖开了鹅的肚子，希望一下获得所有的金蛋，却最终粉碎了自己发财的梦想。

故事讲述的道理很简单，但急功近利，“杀鹅取卵”的事情，在现实中却不乏实例。由于安全产品的特殊性，用户在没有发生事故前，很难了解自己购买的系统是否可靠，而一旦发生了事故，网络安全威胁的复杂和多样，又使他们难以及时判定问题到底出在哪一个环节。而这正为不少厂家留下了可乘之机，他们在生产产品时以偏概全，鱼目混珠；在市场宣传时口若悬河，夸大其词；在实际销售时，更是脱离实际，误导用户。这样的做法虽然在短期内可以获得一定的收益，但却无异于饮鸩止渴，对产业和自身的长远发展，都埋下了深深的隐患。

在安全界中，有一条著名的木桶理论：一套安全体系，不管性能如何优越，技术如何先进，其总体的防御能力，仅仅取决于“最短的那块木板”。寻找和及时弥补这块短板，正是安全技术整合与发展的方向。

同样的，木桶理论也是安全产业发展的精髓。那些贪图眼前利益，急于求成的企业就是产业链中的“短板”，他们不仅自己最终会吞下苦果，而由此给市场带来的恶性竞争和信用缺失，也会使整个安全产业裹足停滞。

网络安全的繁荣怎样才能不仅仅是昙花一现？健康、和谐，充满活力的产业链条如何建立？受到安全威胁的用户怎样才能高枕无忧？寻找这些问题的答案，是我们所有从业人员的使命，也是本期安全专刊制作的初衷。

没有人会是金蛋上的那只鹅，因为这只鹅就是安全产业本身，它需要的是呵护与照料，而不是贪婪和争夺。做到前者，它就会给我们带来源源不绝的财富；而选择后者，则无异于寓言中的农夫，正把这只下金蛋的鹅，放到了切肉的案板上。

张琳

致无畏者：

从工作、娱乐到生活的方方面面…… 我们所在的时代，正因那些无所畏惧的创造者而改变。越来越多的企业和机构已经意识到信息才是最有价值的财产，企业领导者也认识到只有安全、可靠的信息，才能真正创造价值。如今世界各地的公司都在选择互联网安全领域的领先厂商赛门铁克来保护他们的重要信息，因为赛门铁克能够凭借其全面的技术、服务及安全响应，确保信息准确可靠，帮助企业繁荣发展。在这个日新月异的世界，无畏者才能引领一切。您不想加入其中吗？

www.symantec.com.cn

安全的伊索寓言

目录 CONTENTS

马与驴子

从前，有个人赶着一匹马和一头驴子上路。路途中，驴子对马说：「请帮我分担一点我的负担吧。」马不愿意，驴子终因精疲力竭，倒下死了。于是，主人把所有的货物，包括那张驴子皮，都放在马背上。这时，马悲伤地说：「我真倒霉！我怎么会受这么大的苦呢？这全因不愿分担一点驴的负担，现在不但驮上全部的货物，还多加了一张驴皮。」

这个故事告诉我们，不管是为了推卸责任，把货物都推到别人后背，还是为了争夺利益，把货物都揽到自己身上，都不会有好的结果。强者与弱者应相互帮助，分工合作，各自才能更好地生存。

安全产业的天平从来没有像今天这样摇摆不定。

在增加了微软、思科这样的“超级砝码”之后，如何让这架天平重新找到平衡点，成为了网络安全产业最引人关注的话题。

巨人已经踏上了这片土地。对众多的安全专业厂商而言，行动还是沉默，对抗还是合作，不同的立场，不同的策略，不同的方向，最终将决定他们是站在了巨人的肩上，还是

被巨人站在肩上

——网络安全产业竞争新态势

本报记者 张琳

产业篇

“这的确是一片相当广阔的水域，但无论如何也容不下鲸鱼。”

Security Focus 网站新闻编辑 Kevin 的感慨，恐怕也代表了不少安全企业的心声：当微软、思科这样的巨人闯步走进他们苦心经营的玫瑰园时，除了恐惧和无奈，又能怎么样呢？

直接对抗？无异于以卵击石；和他们“坐而论道”？显然更不现实。在一个弱肉强食，以利益为唯一准则的商业社会，我们亟待寻找的，是强弱合作的合理坐标与守则，并以此来绘制安全产业的新版图。

安全产业不安全

“一句话，信息安全行业，狼来了。”在接受记者采访时，天融信副总裁于海波的话让人闻到了安全市场上的硝烟。的确，2005年对于安全产业来说，注定将是风云多变的一年。巨大的市场需求，高速的增长态势，就像是在人群中突然被打开的宝箱，引来了众多的竞争者。众强环伺之下，安全这个饭碗，越来越不好端。

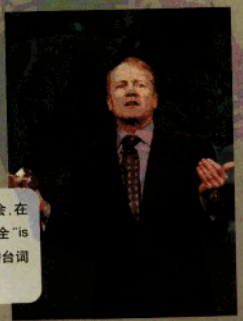
首先让众多反病毒企业坐立不安的就是微软，收购罗马尼亚反病毒厂商GeCAD和反间谍软件公司Giant时，微软在他们的视野中已经变得“形迹可疑”。今年二月，微软又宣布将收购反病毒软件开发商Sybari。该消息公布之后，几家老牌安全厂商如McAfee和赛门铁克的股票应声而跌。

尽管在不同的场合，微软曾多次撇清自己：“我们在反病毒领域主要是和反病

虎！虎！虎！

这就是有钱人的笑脸。在收购了两家反病毒和一家间谍软件公司后，我们强烈建议安全界的人士多多端详这张慈祥的笑脸。浏览器和多媒体播放软件的较量，让我们早已领略了这笑容的威力：“没关系，当你们卖时，我可以送，但看看谁会笑到最后。”

微软 比尔·盖茨



这个指挥家似的手势拍摄于今年二月的RSA大会，在这次安全的盛会上，钱伯斯反复向人们强调，安全“is a networking thing”（是网络的事）。这句话的潜台词就是，“这原本就应该是我们的生意”。

思科 约翰·钱伯斯

趋势科技 CEO 陈怡桦
"坚持专业就可以跑在巨人前面。"

瑞星公司副总裁 毛一丁
"完善与本土化的安全服务将是竞争的最好武器。"

毒供应商紧密合作，并没有意愿去想影响他们本身的业务"。本报相关记者在过去的采访中，也多次从微软的发言人口中印证了这一观点。但是，不少市场观察家认为，微软终将推出自己的反病毒软件，而且时间很可能就在今年晚些时候。

从商业利益的角度来看，这种分析是合情合理的。到今年微软已经年满30了，从90年代开始，它每年的收入都以平均36%的速度增长，年销售额早已达到数百亿美元。然而，近年来其增长速度已明显放缓，主营业务市场趋于饱和，正急于寻找新的业务增长点，而安全恰恰也是近年来增长最为迅猛的一块领域。盖茨在去年就曾表示，计划投资超过60亿美元用于研发，其中最大的部分将投入到安全维护方面中去。

不仅如此，由于微软在电脑操作系统上的绝对优势，一旦迈入安全领地，他完全可以像当初无情地争夺浏览器市场一样，采用和Windows捆绑的方式销售杀毒软件，如果这样，等待很多反病毒厂商的，很可能是"网景"一样的悲惨命运。退一步讲，微软即使在反垄断的大棒下有所收敛，其强大的资金后盾和市场能力也会令大多数竞争对手血染沙场。

就此话题，瑞星副总裁毛一丁在接受采访时表示：如果微软真的大举进入防病毒市场，的确会对现有的厂商造成严重冲击。不过他认为，"微软在安全上的巨大投入，主要是出于用户对其系统安全漏洞的意见，换句话说，是为了维护其操作平台的进一步发展，毕竟这才是他的根基与主业，瑞星一直以来与微软有着非常良好的合作记录，在未来的64位操作系统上，也会有更紧密的合作。如果微软冒着业内众多厂商的大不讳而强行进入安全市场，恐怕是得不偿失。"

的确，从道义上来看，由于目前微软的操作系统和IE等应用软件，是网络病毒登陆并占领电脑的"最佳诺曼底"，用户希望微软做的，就是尽快弥补这些漏洞，提供更安全的系统平台。如果微软反而借此侵入反病毒市场，等于是利用自己的漏洞在赚钱，未免有些"太不厚道"了。难怪Forreste调研公司的分析师认为，微软如果真的推出反病毒产品，将是一种"黑手党式"的行为。

但话又说回来，在商场上，唯一永恒的只有利益，而在利益的驱动下，一切皆有可能。新近到北京访问的趋势科技新任CEO陈怡桦就直言不讳地对记者表示，她上任以来面对的最大外部压力，就是如何应对微软在安全市场上的"小动作"。她认为微软将在今年年底推出个人反病毒产品，而且随后可能进一步染指企业安全市场。

"熔化"的行业？

与微软一样，网络巨人思科也热衷于在安全市场上攻城掠地、大肆搜罗，并且已经取得了相当骄人的业绩。多年稳居网络安全市场的头把交椅。2004年，思科更一举收购四家安全厂商，欲将整个网络安全市场收入囊中。

和微软的"笑里藏刀"不同，思科采用的是"化功大法"。简而言之，就是要把安全这块"甜奶油"，不留痕迹地完全熔化到思科的面包——网络设备中去。

为此，思科提出了新一代的"自防御网络"计划（Self -Defending Network），在有关该计划的白皮书中，记者看到了这样的描述："有一种网络，它的力量能——实现自我保护，更能确保你的业务万无一失；使你的通讯系统融合于一体，更进一步地解放你的生产力使你轻松获取一切信息；这就是你理想中的网络，现在就是开启它的时候！"

这种煽动性的语言对于用户而言，有着不言而喻的吸引力。在采访时，思科公司的网络安全高级顾问喻超向记者表示，越来越多的顾客对思科的这一计划表示了浓厚的兴趣。当然，要实现这样的安全网络，单靠添加一些安全产品是无法实现的，安全将作为一种功能，"熔化"到网络中，成为网络基础建设中的一层。

但是如果安全被整合到网络设备或者系统管理中去，那么它作为一个独立市场，会不会也随之"熔化"呢？

对于记者的这一困惑，喻超表示，"信息安全是否会整合到其它市场将取决于很多因素，但网络安全一定会整合到网络这个统一的市场。正如思科自防御网络所提倡的，网络安全是一个系统级的概念，安全威胁潜藏在网络通信的各个环节之中，各自为政的安全方案在安全威胁面前显得捉襟见肘，所以必须从网络层面就开始全局的考虑安全问题。"

天融信副总裁于海波博士则认为，"技术的融合不仅不会湮灭信息安全市场，反而会推动其快速发展。"于海波谈道"正如一台"应用服务器"的硬件、OS、应用程序不可能完全由IBM或Microsoft独家提供一样，信息安全永远是个永恒的独立主题，它的专业性已经得到业界认可，并将继续作为一个独立市场发展下去。当然在这个发展过程中，会伴随着安全融入到通讯、网络、系统管理中，同时也会出现通讯、网络、系统管理融入到安全设备中。在双方相互融合过程中，信息安全将向更专业、更全面、更深层次发展。"

趋势科技CEO陈怡桦也表达了近似的观点，她认为，安全融合的趋势会进一步推进每个细分领域技术的专业化，而这种专业化反过来会促进安全市场的快速成长。对于顾客来说，安全的应用，以及安全的意义都在一直得到强化，安全市场也将受益于此。

我的地盘听谁的？

卧榻之侧，岂容他人酣睡，更何况这"酣睡"之人势力强大，居心叵测。安全产业原有的各路诸侯面对微软的蠢蠢欲动和思科的大肆扩张，自然心有不甘。

赛门铁克是反映最为激烈的一个。虽然论规模，他无法与两位巨人相提并论，但在网络安全这块地盘上，却是屈指可数的领军人物。作为增长最为迅猛的大型软件企业，赛门铁克的年收入已经超过20亿美金，这使它有资格在巨人的面前指手划脚一番。

为了证明自己的实力，赛门铁克在数据存储这块自己并不熟悉的"平衡木"上，表演了一个360度转体的高难动作。作为软件史上规模最大的一次并购，赛门铁克和Veritas的结合，令不少人大吃一惊。对于这起高达135亿美元的并购案，不少分析家认为，以收购对抗收购并不是明智之举，赛门铁克进入了一个他们并不熟悉，而且发展速度较慢的存储、备份软件业务领域。这将会拖累赛门铁克在安全领域的高速成长。

不过，赛门铁克则坚持认为，自己走在了安全产业发展"最正确的道路"上，其CEO汤普森表示，面对蠕虫、病毒等众多威胁，安全供应商们已经不仅仅是提供防御技术，还应该有能力帮助企业客户存储信息，并在遭受攻击后进行恢复。"我们应该保证信息始终安全、可用。光是保证它的安全是不够的。那样就像把信息锁进保险箱，然后又忘了密码。"

然而，在另外一些安全厂商眼里，赛门铁克的所作所为显然是"不识时务"，在逞匹夫之勇。他们认为，对于专业企业而言，合并不是企业成长壮大的最佳途径，与此对应的，结盟或者合作可能对企业的发展更为灵活有效。

在这方面，趋势科技显然是"广结善缘"的代表。它不仅早早积极加入了思科提出的网络准入计划（NAC），在某些技术领域，更有着非常紧密的合作。趋势科技陈怡桦对记者表示，"今年的5月底到6月初，市场上将会出现由两家共同开发的全新重要产品。"

甚至和潜在的"杀手"微软，趋势科技也"眉来眼去"。去年，它取代了McAfee，为微软全球超过1.87亿的Hotmail用户提供邮件检查，对邮件和其附件进行扫描。在这一合作宣布后，趋势科技的股价在Nasdaq上升了8.5%。

当然，与潜在对手的合作必然会充满风险，但趋势科技认为，只要在专业技术上始终保持领先，"跑在巨人的前面"，就能掌握合作的主动权，"我的地盘还是会听我的"。

深挖洞、广积粮

微软与思科，一"软"一"硬"不断进逼，使得安全市场像一截两头燃烧的蜡烛，留给传统专业安全厂商的时间已经不多。

面对日益严峻的竞争态势，天融信公司副总裁于海波表示，唯一的出路就是走专业化道路，在信息安全领域深挖洞、广积粮，成为安全领域领导企业。

此外，从服务发展趋势来看，专业信息安全服务前景广阔，大有可为。网络配置了安全产品，但没有服务，那么安全设备将形同虚设，安全服务是信息安全的重要组成部分已经形成共识。安全服务市场将成为信息安全市场新的增长点，优质的安全服务将给供应商带来好的品牌收益和经济收益，很有可能成为今后信息安全产品市场竞争的准入证和制胜法宝。

天融信副总裁 于海波
"在信息安全领域要'深挖洞，广积粮'。"

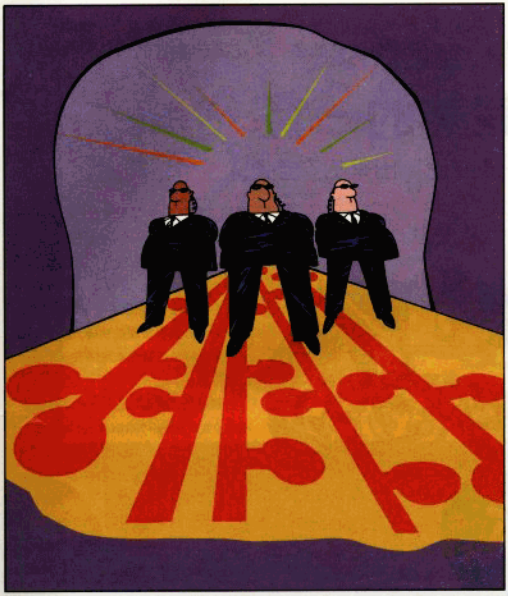
思科网络安全高级顾问 喻超
"网络安全一定会整合到网络这个统一的市场。"

瑞星副总裁毛一丁也认为，反病毒行业其实最重要的一块就是对用户的服务，能不能及时捕捉到病毒并尽快提供升级响应，是反病毒企业致胜的关键一环。另外，不少用户由于缺乏安全知识和专业人员，需要厂商提供最直观的安全服务，在日本等国，这种方式就非常流行。瑞星也将借助自己的技术和本地化优势，在这方面有所作为。

专业安全厂商的生存与发展，还将面临的一个重要挑战就是无可回避的整合浪潮。其中包括：用户需求的整合、技术与功能的整合、产品与服务的整合、架构体系的整合、安全业务与网络和基础设施管理的整合。

所有这些整合，每一步都将牵扯到产业生态链的不同环节、牵扯到一家家具体的安全企业、牵扯到或强或弱的"马"和"驴"。因此，让我们回到前面的寓言故事，再一次强调合作对于这个行业非同寻常的意义。因为只有所有企业的共同努力，才能背负起安全产业的未来。

IT产业无人永生，生存的挣扎使这块土地永远不会平寂。虽然"马"和"驴"的争执与摩擦在所难免，但我们仍企盼着一个坦诚、和谐的产业环境能尽快建立，否则，当硝烟散尽，网络安全的战场上可能将只剩下病毒与黑客的笑容。



您有多重视网络安全？

- **SSL VPN：**我们的SSL VPN设备拥有全球42%*的市场占有率，被公认是安全远程接入及安全外联网络领域的全球领导者 —— 无需安装客户端软件、无需更改内部服务器，也无需提供成本高昂的维护服务及桌面系统支持。

- **IPSec VPN：**Juniper网络公司的IPSec VPN提供了具备故障恢复功能的解决方案，包括能够在少于一秒钟内完成故障切换的状态高可用性。利用这个解决方案，您可以放心地一直保持连接。

- **状态防火墙（系统）**提供接入控制和带数据包深层检测的验证功能，可确保您的网络接入点及应用的安全，以使您的业务畅通无阻。

- **入侵检测与防护（系统）**使您更有效地防止应用层攻击，甚至在这种攻击被确定为恶性攻击之前就能预先做出反应。

- **安全路由（系统）：**Juniper网络公司的企业路由平台可为您的网络提供服务供应商级的安全性、质量及性能。

*Q4 '04, Infonetics Research

您的企业依赖网络系统，而您的网络系统每天都面临着日益严峻的安全威胁。此时，您需要Juniper网络公司为您提供彻底的安全保障。

Juniper网络公司的产品系列提供从网络层到应用层的安全性。利用强劲的系统设计和定制的硅所提供的卓越性能，我们能提供符合您业务要求的解决方案。

Juniper NETWORKS

Juniper your Net.

www.cn.juniper.net www.juniper.net

Juniper 网络公司（中国）办事处

北京市东城区东长安街1号
东方经贸城西三办公楼15层1508室
邮政编码：100738
电话：8610-8518-2826 传真：8610-8518-2826

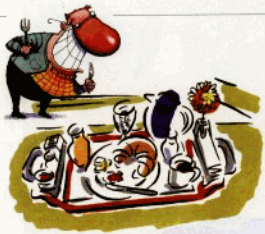
上海市浦东中路333号
银亿广场1102-1104室
邮政编号：200021
电话：8621-6141-5000 传真：8621-6141-5001

广州市天河区体育东路118号
财富广场南塔15楼1501室
邮政编号：510620
电话：8620-3886-0668 传真：8620-3886-0636

在IT技术产业中，思科是真正的“美食家”，他有胃口、有眼光，最关键的是，他花得起这样的钱。

完美的一餐

——“吃”出来的安全巨人



依靠不断的进食，思科获取了不同技术领域的“营养精华”，迈入网络安全行业后，我们同样看到了这一做法的延续。2003年底，思科正式提出了自防御网络（Self-Defending Network，SDN）计划，为达到这一目标，随后的2004年，思科吃下了一顿丰盛的“安全套餐”。而这完美的一餐，不仅使得思科的自防御网络计划逐步从理想变为现实。同样的，这也是我们理解网络安全技术动向，以及学习企业收购策略的最佳读本。

“开胃菜”是来自美国加州的Twingo Systems公司，它帮助思科解决了SSL VPN的安全难题，利用Twingo的虚拟安全桌面技术，可以安全连接到敏感企业网的计算机上，建立虚拟桌面环境，会话期间往来的信息被加密存储到虚拟桌面，在会话结束时自动从机器上删除，从而保护用户的隐私和安全。思科通过此次收购，可以增强连接设备的安全性。

“副菜”是已经在DDoS防护领域颇负声名的Riverhead Networks公司，我们知道，分布式拒绝服务攻击（DDoS）一直是网络的灾难，它是目前网络黑客最常使用也是最具破坏力的武器。Riverhead公司自2001年以来一直专注于DDoS技术的发展，其智能化DDoS防护系统由于采用了被称为MVP的专利技术，再加上专用芯片，使得该防护系统效率极高。Riverhead公司的产品2002年一经推出，很快就得到电信运营商、门户网站、在线游戏公司、在线支付公司的青睐。当然，盯上它的还有思科。在花费了不到3个月的时间后，思科便闪电般的将它吞进了肚中。

接下来的“主菜”同样是来自加州的Perfigo公司，该公司的集成化网络准入控制解决方案，可以为网络提供终端策略分析、兼容性和权限执行等功能，这无疑非常对思科的胃口，因为这恰恰是思科自防御网络中重要组成部分——NAC（网络准入控制）所需要实现的功能。同时，该解决方案也将是思科未来网络安全发展的基础组件之一。

最后的“甜点”是2002年底才刚刚成立的Protego Networks公司。Protego开发了一整套高性能、可扩展的网络安全设备。这些设备能够和现有的传统网络相结合，具有网络事件监控、网络智能、上下文相关、矢量分析、异常监测、热点辨认以及自动恢复功能。企业网络配备Protego网络智能设备后，能够更加迅速精确地消除网络攻击并自我恢复，维护网络正常运转，这些正好是对思科自防御网络安全战略的进一步完善。

为了给上述这顿网络安全大餐买单，思科一共花费了1亿8千3百万美金（详见附表），对于思科的胃口来说，这只能算是正常的食量。2005年思科还将吞下什么，我们拭目以待。

思科的菜单（2004年思科网络安全领域收购行动一览）

上菜顺序	菜品（公司名称）	特色（主导产品或优势技术）	生产日期（成立时间）	进餐时间（收购日期）	价格（收购价）
开胃菜	Twingo Systems公司	虚拟安全桌面技术，解决SSL VPN安全问题		3月	500万美元
副菜	Riverhead Networks公司	DDoS攻击防护器，有效防范DDos攻击	2000年	4月	3900万美元
主菜	Perfigo公司	SecureSmart和Clean Machines，使NAC准入智能化	2002年	10月	7400万美元
甜点	Protego Networks公司	智能化安全监控和管理	2002年	12月	6500万美元

一只眼睛的鹿

有头瞎了一只眼的鹿，来到海边吃草，他用那只好的眼睛注视着陆地，防备猎人的攻击，而用瞎了的那只眼对着大海，他认为海那边不会发生什么危险。不料有人乘船从海上经过这里，看见了这头鹿，一箭就把他射倒了。他将要咽气的时候，自言自语地说：「我真是不幸，我防范着陆地那面，而我所信赖的海这面却给我带来了灾难。」这故事告诉我们，事实常常与我们的预料相反，以为是危险的事情却倒很安全，相信是安全的却更危险。

天真，对一个人而言，也许是好事；对于一家企业，则意味着危险；对一个产业来说，更是一场灾难。

多次的权威机构调查结果告诉了我们安全的 80/20 法则：超过80%的安全威胁，源自于企业内部。然而，仍有不少人在建立安全系统时，“天真”地假设内部安全的，将几乎所有的安全投资都用在“防外”的措施上，这种盲目的“安全感”最终会让企业吞下苦果。

安全的最高境界不是产品和技术，而是管理。但这注定是最难攻克的堡垒，因为对手不是别人，就是我们自己。

安全管理之“天下无贼”

本报记者 张琳

“傻根”式的企业

在安全的问题上，不自信往往是一件好事情，尤其是如今的计算机犯罪已经变得越来越穷凶极恶。但是，仍有不少企业在内部的安全问题上盲目乐观，这种如同《天下无贼》中“傻根”似的天真，通常“后果很严重”。

早在2003年，就有媒体报道过，亚信等企业给客户的技术解决方案及技术文档被泄密，这些重要的商业文件甚至被制作成光盘，出现在中关村的盗版市场上。从内容上看，单是亚信公司被非法收录、汇集的解决方案和技术文档就有“中国网通运营维护支撑系统”、“北京电信公众IP网络集成工程规范书”等全部WORD文档，每个项目都是价值千万元以上。而和亚信有同样遭遇的，还有不少国内外大型IT企业，内容涉及整体解决方案、流程、规划、技术白皮书等，很显然，如此完整详尽的资料，相信一定有公司内部的人员参与泄密。事件发生后，这些公司都加强了内部信息系统的安全管理。

随着信息化发展的进程，网络信息系统和企业的核心业务关联性越来越大，信息的商业价值也水涨船高。这使得越来越多别有用心的人铤而走险，而通过企业的内部获取机密信息，往往是一条最佳“捷径”。

虽然，很多公司在信息安全上投入重金，其防护系统从产品到技术都更加先进，企业对于安全的自信心也得到加强，但是，安全管理的滞后仍然是一个致命的安全漏洞。

美国《Network World》的调研也基本上证实了这一观点。2004年9月，在一次对263家企业的调查结果表明，尽管65%的企业对安全措施感到有信心或很有信心，认为自己能够很好地防范日常的威胁，但结果是，这些企业每年因计算机入侵遭受的损失为1.78亿美元，而且公司越大，损失也就越大。这些公司中有118家的员工数量低于500人，它们的总损失数额为1600万美元，而另外145家员工数量为500人或500人以上的，总的损失达到了1.62亿美元。

企业内部人员对信息安全从来并且可能永远都是最大的威胁。由于内部人员比任何外人都更了解企业的网络。如果有人心怀不满，可以很容易把公司的重要商业信息带走，或者把它泄露出去，对企业造成损害。通常企业都比较信任内部的员工，差不多两年前，多数的安全设备根本不对企业网络内部的情况进行监视。企业内部的每一个人都得到了充分的信任，可以在网络中随意游走，毫无限制。目前，越来越多的企业意识到了这类威胁，大多数网络安全设备也开始同时监视企业内部和外部的情况，并且对那些可疑的活动类型进行阻止或提出警告。但是，对企业而言，内部的威胁仍然是不可轻视的最大安全隐患。

阴影中的凶手

对于企业内部的信息安全管理，还有一个令人头痛的问题，那就是在所造成的恶果显现之前，企业很难发现犯罪线索。

计算机网络犯罪通常十分隐蔽，并没有发生任何可见的偷盗行为。计算机虽然仍然位于服务器机房里，但犯罪犯却可能已经通过复制或修改数据的方式窃取了信息，并利用这些信息来进行身份盗窃、泄露商业秘密或专有代码。

另外一个令人不安的趋势是：很多信息系统的入侵者并不盗取数据，而是

对其完整性进行修改。如果企业内部员工因商业利益或其他原因对公司怀恨在心，那么他破坏该公司的数据库，所造成的危害就会远远大于简单的盗取数据。而且这种行为也更难被发现。比如对企业日常商业贸易中的时效性数据进行修改，并使其失去连贯性，那么企业管理者就根本无从知道到底发生了什么，什么才是正确的内容。这种行为很可能影响企业未来的关键决策，造成的危害后果几乎是无法估量的。

Unisys公司安全顾问表示："那些年轻的、经验不足的人进行计算机犯罪的目的，通常只是因为觉得有趣或者想让自己臭名远扬。但公司内部的信息安全犯罪通常怀有商业目的，因此也更加专业，他们通常对企业信息系统的弱点了如指掌，完全可以以神不知，鬼不觉的方式访问、删除或修改信息。"

企业内部的"凶手"能够成功躲在阴影中的另一个原因，就是大多数企业在碰到类似的问题后，都不愿意报案。

CSI/FBI最近进行的研究表明，只有20%的企业向执法部门报告了安全防线被攻破的事实，而在2001年，这一比例为36%。

对信息安全犯罪隐而不报的原因有很多，有些企业内部就有此类的相关规定，害怕由此带来更多的负面影响；有些企业则担心消息被外界知晓后，会影响股票价格下跌；还有一些企业的相关管理层害怕承担责任，不仅不报，反而会替入侵者的行为进行掩盖。

在相关的调查中，一位受访者说："我们的企业也曾发现来自内部员工的攻击。但我们没有相应的资源来解决这些问题。我的工作只是通过各种技术手段确保网络的正常运转，而通过法律进行侵权诉讼根本不在我的职责范围内。"

据统计，能够如实报告信息系统受到来自内部威胁的公司只是"冰山上很小很小的一角"。而且，有些行业，如金融、证券等，无论如何也不会对外界报告此类事件，但很显然的是，它们恰恰都是网络计算机犯罪攻击的最佳目标。

用管理进行反击

"天下无贼"是一个难以企及的梦想，但通过有效的安全管理，最大限度地减少内部安全威胁则是可行的。

企业首先要做的，就是在专业公司的帮助下进行安全审查，清楚地了解企业网络安全的体系与问题。因为实际上，很多企业并不是采用的安全技术本身有什么问题，而是技术的部署与实施存在漏洞。这种安全审查应该反复多次并成为习惯，因为即使被认为安全的环境，也会随着时间发生变化。

拿无线接入来说，目前许多公司都已经采用了开放式的无线接入技术，但正因为这种接入方式的开放性，就会被一些心怀叵测的人加以利用。当然，出于安全风险的考虑，你也可以在企业安全策略中禁止在内部网络中使用无线技术。不过，你仍然无法保证员工会言听计从。由于眼下无线设备的价格非常便宜，你的员工只要花几百元就能买到这种无线设备，然后把这东西接入企业网络，这种举动无疑相当于在企业的安全体系中插出一个洞，只要一名员工就能够以非常"轻松廉价"的方式完成这种"破坏性"的部署。也许一台价值几百元的设备就能够让投资上千万的安全架构毁于一旦。更可怕的是，公司

的系统管理员根本没有什么办法来阻止此类活动。

所以，网络技术的发展也会带来更多的安全挑战，管理的意义，就在于随时都不能掉以轻心。

美国《Network World》的调查中可以让我们稍感欣慰的是，目前在企业中进行安全审查的比例，比三年前要高得多，但形势依然严峻：60%的受访企业每年只进行两次或更少的安全审查，绝大多数企业进行审查的次数只有一次。在国内，我们也咨询了相关的专业安全厂商，他们称国内企业主动进行这类安全审查的更是少之又少，这不得不引起我们的警惕。

天融信公司的王亚平表示，防范来自企业内部的安全威胁，首先要建立规范的信息化管理系统，并且具备基本的安全保障系统，比如企业总部与分支机构的网络互联一定要使用VPN；二是要有安全管理制度体系，并且制度能够有效地执行；三是，企业领导对信息安全问题的高度重视。在上述三点中，最难的在于如何有效地制定并执行安全管理制度体系，这涉及到企业的管理风格，业务模式与对信息安全的重视依赖程度，是最难把握的一个环节。

虽然我们非常清楚地知道企业内部人员的危险程度有多高，但是，内部人员的犯罪活动是无法预测的。谁都不可能知道哪些员工会在什么时间干出伤害公司利益的事情，人性本身的变化是最难控制与防范的。当然我们也可以借助一些技术工具，比如员工行为管理（EIM）、客户端安全管理等等。

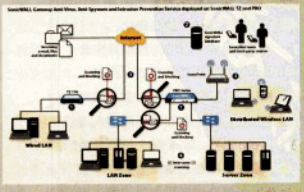
这类管理工具通常包括两部份，一部分是员工网上行为管理（EIM），另一部分是员工桌面行为监测。它一般在Internet应用层、网络层对信息控制，对数据根据EIM数据库进行过滤；定制互联网访问策略，根据用户、团组、部门、工作站或网络设置不同的互联网访问策略。当然，这类工具在应用时还要考虑员工的隐私权等问题。

此外，安全服务也是解决企业内部安全管理的有效手段之一。从用户的角度来看，信息安全服务能带来的实际好处包括：弥补用户人力的不足，弥补用户技术的不足，弥补用户信息的不足，弥补用户管理思想的不足。这些服务内容主要通过服务团队，特别是一线人员传递到用户的手中，服务人员的技术技能和态度将直接决定用户的收益。针对内部的安全威胁，定期的安全服务更可以为用户提供更多的手段去保障业务的正常进行。

总之，既然我们愿意为20%的安全威胁花费重金，又有什么理由对80%的风险视而不见呢？

SonicWALL 深度包检测引擎的功能和特点

防火墙技术经历了从第一代的包过滤防火墙，第二代的应用代理防火墙到第三代的全状态检测防火墙。各种入侵和攻击也从针对TCP/IP协议本身弱点的攻击转向针对特定系统和应用漏洞的攻击，这些攻击和入侵手段封装在TCP/IP协议的净荷部分。传统的防火墙，包括第三代全状态检测防火墙，对这些入侵和攻击手段无能为力，因为它们只查TCP/IP协议包头部分而不检查数据包的内容。病毒，黑客入侵及间谍软件正在给互联网用户造成巨大的损失。



为此，美国SonicWALL公司推出了全新设计的UTM一体化网络安全设备。UTM通常包括防火墙/VPN，网关防病毒和IPS。SonicWALL采用独一无二的逐个包扫描深度包检测引擎（SonicWALL DPI引擎，美国专利申请中），无需对数据包重组及对文件进行缓存就可以实现对病毒和入侵的扫描和防护，彻底消除了传统网关防病毒设备对同时下载的文件数目和文件的大小的限制。SonicWALL UTM设备能够并行扫描超过50种协议上的近25000种病毒，检测并阻断近2000种入侵威胁，包括针对对VoIP协议漏洞的攻击。

SonicWALL还支持对100多种即时消息(IM，如MSN、QQ)和对等应用(P2P，如BT下载、eMule下载)的通信控制。能够扫描NetBIOS over TCP/IP，防止病毒通过Windows文件共享进行扩散。同时，SonicWALL解决方案还可以限制带有宏的Office文件、密码保护的压缩文件和“加壳”的可执行文件的传输。

采用DEA架构，SonicWALL的安全设备做到了每个小时自动更新病毒签名库和入侵签名库。此外，SonicWALL的UTM设备即将支持反间谍软件功能，通过简单的软件升级，现有的网关防病毒和IPS用户可直接享用反间谍软件服务。