启明星辰网络安全解决方案

启明星辰公司自 1996 年成立以来，已经开发了黑客防范与反攻击产品线、采用国际著名厂商芬兰 F-Secure 公司杀毒技术形成的网络病毒防杀产品线、以网站安全扫描与个人主机保护为代表的网络安全管理产品线，以及几大产品线之间互动的网络资源管理平台，成为具有自主知识产权、覆盖防病毒和反黑客两大领域的高科技含量的网络安全产品研发与生产基地。启明星辰公司产品均获得了《计算机信息系统安全专用产品销售许可证》，《国家信息安全产品测评认证证书》和《军用信息安全产品认证证书》，在政府、

银行、证券、电信和军队等领域得到了广泛的使用。

网络安全产品链

相关方案包括：

天阗(tian)黑客入侵检测系统

天镜网络漏洞扫描系统

天衡(heng)安防网络防病毒系统

Webkeeper 网站监测与修复系统

安星主机保护系统

天燕智能网络信息分析实录仪

C-SAS 客户化安全保障服务

天阗(tian)黑客入侵检测系

(阗：在中国古代有“和田美玉”之意，坚固圆润，异彩流光，可以补天。)

一般认为，计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击 3 个方面。目前，人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现，而随着 Internet 的发展。现代黑客则从以系统为主的攻击转

变到以网络为主的攻击，新的手法包括：通过网络监听获取网上用户的帐号和密码；监听密钥分配过程、攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 Unix 操作系统提供的守护进程的缺省帐户进行攻击，如 Telnet Daemon，FTP Daemon,RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 Sendmail，采用 debug,wizard,pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等等。目前，已知的黑客攻击手段已多达 500 余种。

入侵检测系统

防火墙与 IDS

谈到网络安全，人们第一个想到的是防火墙。但随着技术的发展，网络日趋复杂，传统防火墙所暴露出来的不足和弱点引出了人们对入侵检测系统(IDS)技术的研究和开发。首先，传统的防火墙在工作时，就像深宅大院虽有高大的院墙，却不能挡住小老鼠甚至是家贼的偷袭一样，因为入侵者可以找到防火墙背后可能敞开的后门。其次，防火墙完全不能阻止来自内部的袭击，而通过调查发现，70%的攻击都将来自于内部，对于企业内部心怀不满的员工来说，防火墙形同虚设。再者，由于性能的限制，防火墙通常不能提供实时的入侵检测能力，而这一点，对于现在层出不穷的攻击技术来说是至关重要的。第四，防火墙对于病毒也束手无策。因此，以为在 Internet 入口处部署防火墙系统就足够安全的想法是不切实际的。入侵检测系统(IDS)可以弥补防火墙的不足，为网络安全提供实时的入侵检测及采取相应的防护手段，如及时记录证据用于跟踪、切断网络连接，执行用户的安全策略等。

IDS 概念解析

入侵检测系统全称为 Intrusion Detection System，它从计算机网络系统中的关键点收集信息，并分析这些信息，检查网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门。IDS 主要执行如下任务：

1. 监视、分析用户及系统活动。
2. 系统构造变化和弱点的审计。
3. 识别反映已知进攻的活动模式并向相关人士报警。
4. 异常行为模式的统计分析。
5. 评估重要系统和数据文件的完整性。
6. 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

一个成功的入侵检测系统，不仅可使系统管理员时刻了解网络系统，还能给网络安全策略的制订提供依据。它应该管理配置简单，使非专业人员非常容易地获得网络安全。入侵检测的规模还应根据网络规模、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和报警等。IDS 分类入侵检测通过对入侵行为的过程与特征进行研究，使安全系统对入侵事件和入侵过程作出实时响应。

入侵检测系统按其输入数据的来源来看，可以分为以下两种：

1.基于主机的入侵检测系统：其输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。

2.基于网络的入侵检测系统：其输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。

IDS 功能结构

总体来讲，入侵检测系统的功能有：

1．监视用户和系统的运行状况，查找非法用户和合法用户的越权操作。

2．检测系统配置的正确性和安全漏洞，并提示管理员修补漏洞。

3．对用户的非正常活动进行统计分析，发现入侵行为的规律。

4．检查系统程序和数据的一致性与正确性。如计算和比较文件系统的校验和能够实时对检测到的入侵行为进行反应。

天阗概述

天阗正是适应入侵检测这一实际需求的产物。简而言之，天阗能够收集并分析计算机系统和网络中的关键信息，检查系统和网络中是否有违反安全策略的行为和遭到袭击的迹象。它是启明星辰公司开拓国内的网络安全市场，并具有自主知识产权的战略性产品。启明星辰公司已为此投入了相当大的资源，并取得了显著的成果，启明星辰还将继续努力，保持在该领域技术上的领先优势。

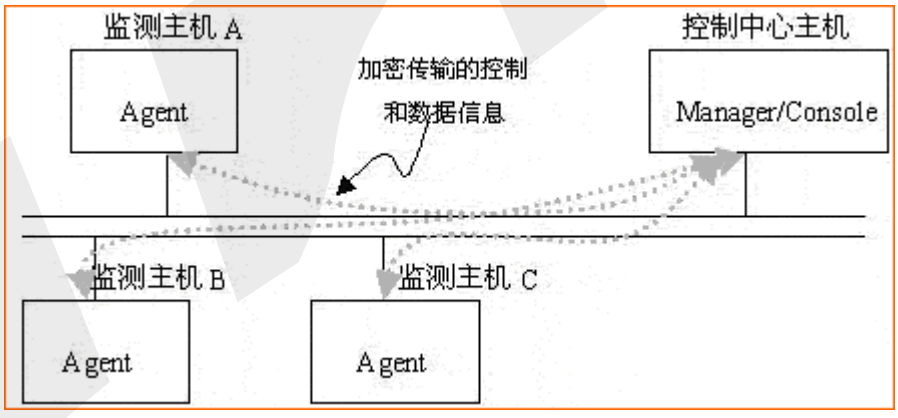
天阗分主机版和网络版。主机版天阗是基于主机的入侵检测系统，它监视系统的运行状况，监视系统上用户的操作，对用户的活动进行审计和分析，对系统程序和数据的一致性和正确性进行检查；网络版天阗是基于网络的入侵检测系统，监视网络的运行状况，分析网络上的可疑行为，对正常及非正常的活动进行审计和分析，向网络控制台实时报警，并且能根据预先配置的策略自动对攻击作出反应。

主机版天阗

主机版天阗是基于主机的入侵检测系统，以下称为天阗主机入侵检测系统。

天阗主机入侵检测系统目前支持 Solaris 7（SPARC）系统。他能自动、实时的入侵检测和响应系统。它能够实时监控系统，自动检测可疑行为，分析来自主机内部的入侵信号。在系统受到危害前发出警告，实时对攻击作出反应，并提供补救措施，最大程度地为主机系统提供安全保障。

天阗主机入侵检测系统分为两个部分：控制中心和探测引擎。探测引擎端负责将审计数据和日志记录作简单的处理后，形成安全相关事件后，上报控制中心（见下图）。



控制中心负责，①制定入侵监测的策略；②收集来自多台主机的上报事件，综合进行事件分析，以多种方式对入侵事件作出快速响应。

系统特点

内置多种预定义策略，并允许用户添加修改策略；

具有自动/手动两种启动模式；

除去由控制中心集中管理之外，还提供基于命令行的管理工具；

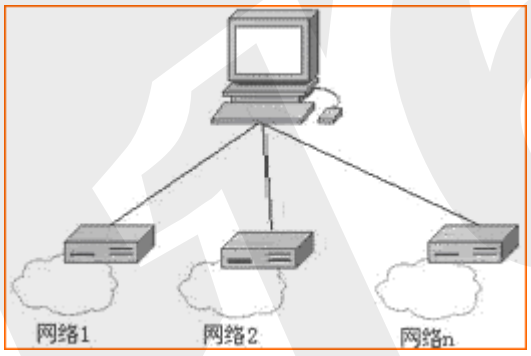
具备多种安全的自我保护功能，防止探测引擎被恶意破坏。

网络版天阗

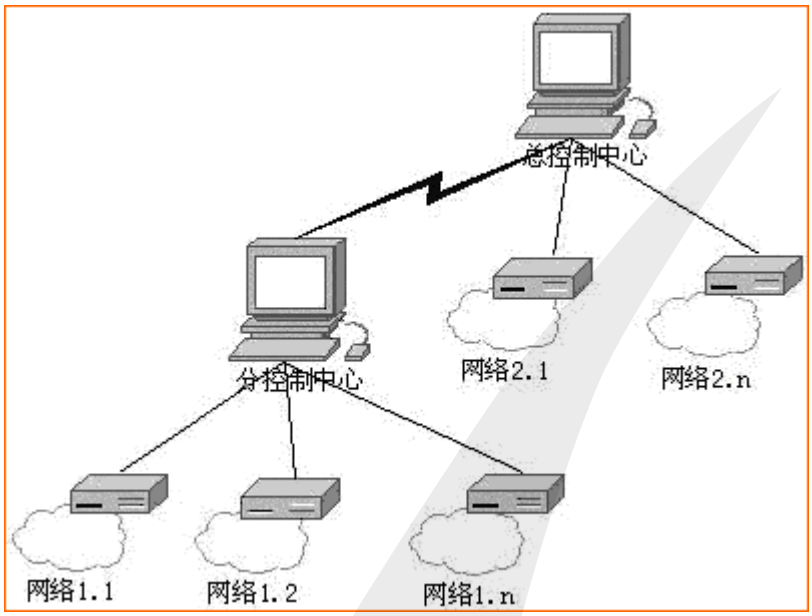
网络版天阗是基于网络的入侵检测系统，以下称为天阗网络入侵检测系统。

天阗网络入侵检测系统是通过监视网络中的数据包来发现黑客的入侵企图，它可以运行在一台单独的计算机上监视整个网络的信息。

天阗网络入侵检测系统是一种分布式的网络入侵检测系统，可以适用于任何规模的网络。无论是小型局域网还是跨地区的城际网络，都可以自由，灵活的来部署天阗。



多个局部预警网络可以相互联系，按照一定的规则构建成一个多层次，分级管理的大规模的预警网络。



网络探测器是预警系统中检测部分的核心。通过对网络进行实时监听，收集网络上的信息，并对这些信息进行实时的分析，看是否对被保护的网络构成威胁，然后按照预先定义的策略自动报警，阻断和记录日志等。

控制中心是预警系统的管理和配置工具，同时，它也接收来自网络探测器的实时报警信息，控制中心还提供了将实时报警信息转发至邮件信箱的功能。

控制中心可以编辑，修改和分发下属网络探测器和下属分控制中心的策略定义，给下属网络探测器升级事件库。

系统特点

内置了多种预定义策略，并允许用户添加修改策略；

防火墙进行联合行动，阻断任何非法连接；

实时显示分析结果；

开放式事件特征库，任何人都可以自行定义和添加特征事件；

包含一个报表分析软件，事后可对日志进行二次分析；

网络流量分析，可以帮助分析网络故障；

提供固化版本的网络探测器，即插即用，方便安装；

系统运行环境

天阗主机版

探测引擎：Solaris 7 (SPARC)

控制中心：Windows 2000

天阗网络版

探测引擎：RedHat Linux 6.1

控制中心：windows 2000

天镜网络漏洞扫描系统

（镜：古有“明镜高悬”一说，即可以照人，又可以耀物，真实反映客观现状，拾缺补漏。）

漏洞检测和安全风险评估技术，因其可预知主体受攻击的可能性和具体的指证将要发生的行为和产生的后果，而受到网络安全业界的重视。这一技术的应用可帮助识别检测对象的系统资源，分析这一资源被攻击的可能指数，了解支撑系统本身的脆弱性，评估所有存在的安全风险。

天镜网络漏洞扫描系统就是这一技术的实现，她包括了网络模拟攻击，漏洞检测，报告服务进程，提取对象信息，以及评测风险，提供安全建议和改进措施等功能，帮助用户控制可能发生的安全事件，最大可能的消除安全隐患。该系统具有强大的漏洞检测能力和检测效率，贴切用户需求的功能定义，灵活多样的检测方式，详尽的漏洞修补方案和友好的报表系统，以及方便的在线升级。

网络可能存在漏洞

系统设置配置不当使得普通用户权限过高

员由于操作不当使得系统被安装了后门程序

系统本身或应用程序存在可被利用的漏洞

对于网络安全来说，安全性取决于所有安全措施中最薄弱的环节，而上面我们所讨论的问题，就是网络的薄弱之处，也是最容易被黑客利用来侵入系统，给我们造成损失的环节。

总体特点

可以动态地分析目标系统的安全脆弱性

根据不同的对象类型，自动寻找匹配的扫描策略进行下一步的分析扫描。

远程在线升级

远程下载升级模块，自动完成升级过程

灵活的策略配置

可按照特定的需求配置多种扫描策略和扫描参数，实现不同内容、不同级别、不同程度、不同层次的扫描。

多种形式的报表

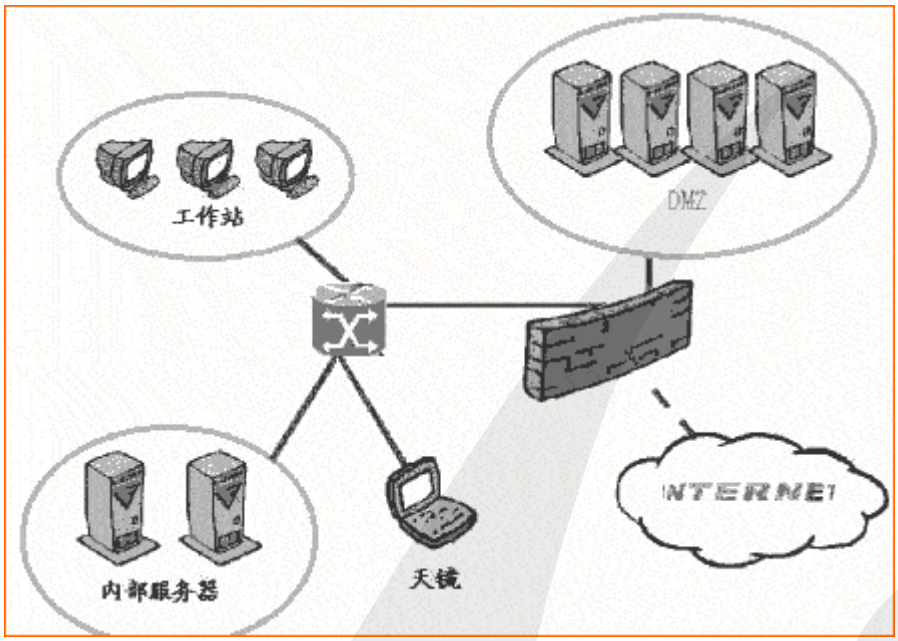
全面详细的分析报告能力，可根据用户的不同需求提供不同层次的报告，并提供安全补丁供应商的热连接，快速及时的修补漏洞。

实用的模拟攻击工具

系统提供用于测试的模拟攻击工具，较好反映了黑客实际攻击的必经之路，同时对被测试系统的测试力度可控，不会为系统带来危害。

合理的结构化设计、模块的继承性，使得系统具有很大的可扩展空间

应用结构



镜漏洞扫描系统

网络版天镜可扫描任何基于 TCP/IP 的网络主机，无论网络核心是采用 FDDI、ATM 还是千兆以太网，只要目标主机支持 TCP/IP 协议，就可对其进行扫描。

1、系统扫描内容：

报表应用界面

Web 服务

FTP 服务

守护进程

电子邮件服务

CGI-BIN

浏览器设置

RPC 攻击

特定的强力攻击选项

拒绝服务攻击检测

安全区检测

NT 用户策略

NetBIOS

NT 注册表

NT 服务

SNMP

缓冲溢出检测

NFS 检测

IP 欺骗

特洛伊后门程序检测

共享/DCOM 类

NT 服务类

2、产品优点：

全自动、大规模的扫描任务

每次最大可扫描多达 255 台主机，扫描任务一经启动，无需人工干预；

多线程扫描

保证了扫描任务的高效性和稳定性；

定时扫描机制

保证充分利用网络空闲间隙进行网络安全状况评估；

丰富的漏洞检查列表

共计 25 大类 600 多种漏洞检测，并跟进最新的漏洞，将其加入到漏洞库中，大大减少用户系统中的隐患； 方便灵活的用户自定义策略

系统内置“强”、“中”、“弱”三种扫描策略，用户也可以根据需要自定义扫描策略并进行储存，就用户所关心的项目进行重点检测；

提供修补漏洞的解决办法

在报告漏洞的同时，提供相关的技术站点和修补办法，方便管理员进行管理；

实用的模拟攻击工具

可直观反映系统的脆弱性；

人性化的扫描报表

系统对于被检测主机的漏洞危险级别利用红、黄、绿分别对高、中、低风险进行标示，同时对于被选中的主机检测信息进行突出显示，方便管理员的查询管理；

分级、灵活的预定义报告

扫描结果可以生成三种不同类型的报告，供领导、技术主管、技术员等不同级别的人审阅；

远程在线升级

远程下载升级模块，自动完成升级过程；

合理的结构化设计

模块的继承性，使得系统具有很大的可扩展空间；

详尽的安全解决方案

帮助用户在了解网络安全状况的情况下得到详尽可行的的解决措施。

天衢(heng)安防网络防病毒系统

（衢(heng)：草木旺盛、欣欣向荣之意，是一种万物和谐、均衡发展的状态）

计算机病毒从 1983 年被首次发现以来，在将近 20 年的发展过程中，在数目和危害性上都有着飞速的发展。近几年计算机病毒问题已经越来越受到计算机用户和计算机反病毒专家的重视，美丽莎、CIH、爱虫、happytime、funlove、Sircam、code red……这些都已经成为大家耳熟能详的计算机病毒名称。虽然很多用户已经使用了防病毒产品，但是日益增加的病毒事件和企业的分布式趋势使得病毒防护和防病毒产品的管理越来越难；另外，防病毒产品需要不断更新其病毒定义库，很多用户由于忘记更新他们防病毒产品的病毒定义库而使得现有的防病毒系统形同虚设。

天衢安防网络防病毒系统是启明星辰公司推出的国产化防病毒产品，它使用了国际著名的杀毒软件厂商 F-Secure 公司的杀毒技术。

天衢安防防病毒系统是世界上最综合的集中式管理的防病毒系统，适用于企业的各类计算系统，包括移动设备、工作站、服务器、防火墙和网关。对于那些正在迅速迈向分布式的、移动的网络环境的企业，天衢安防提供了最强大的病毒以及恶意代码防范功能，无论是对固定用户还是移动用户，均实现了最大的系统可用性和数据安全性。

目前，天衢安防网络防病毒系统已在金融、证券、电信、大型网站及国家政府部门、企事业单位得到广泛应用，其集中式管理、优秀的病毒查杀能力，以及全自动升级技术得到了用户的广泛好评。在 2000 年 10 月公安部国内外网络防病毒系统测试评比中获得最高级别产品。

主要功能

实时病毒扫描；

手动扫描；

报警及病毒事件处理；

扫描 ZIP、LZH、ARJ、RAR 等多种压缩文件，并支持交叉扫描；

对最终用户透明；

持与 SNMP、Microsoft SMS 及 IBM Tivoli TME10 等网管软件结合；

CheckPoint Firewall 容协议防火墙；

天更新病毒定义库。

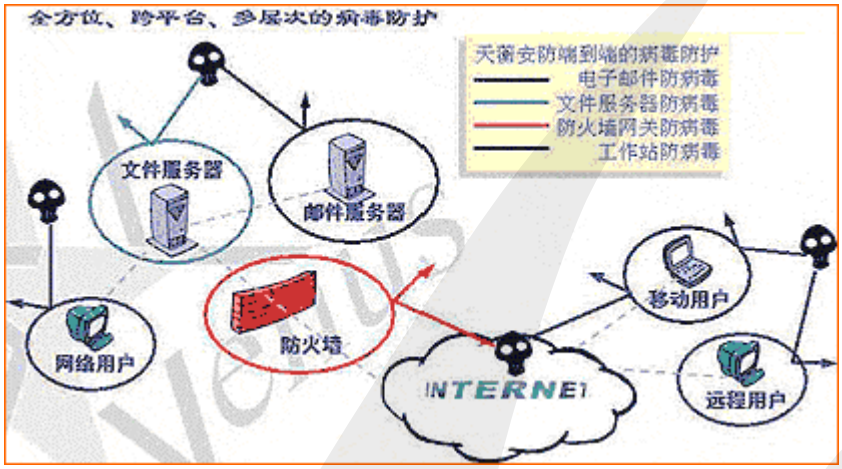
主要特点

全方位多层次的病毒防护能力

天衢安防网络防病毒系统在三个层面上制止病毒的肆虐：一在工作站，这是大多数发生

病毒感染的地方；二在服务器，防止病毒扩散；三在防火墙及网关，防止病毒从网络进入企业内部。

天衢安防网络防病毒系统支持目前多种操作系统平台，包括 Windows 2000、WindowsNT、Windows 95/98、DOS、Linux、OS/2 等。



集中安装和管理

全球唯一通过策略管理器（Policy Manager）来进行集中管理和配置的防病毒产品。策略管理器包括三个关健部件：

<B.管理台（ADMINISTRATOR）< b>

管理台是基于 Java 的应用程序，可以跨不同平台上运行，提供集中式的管理控制台，以保障网络中被管理的主机安全。

管理服务器（Management Server）

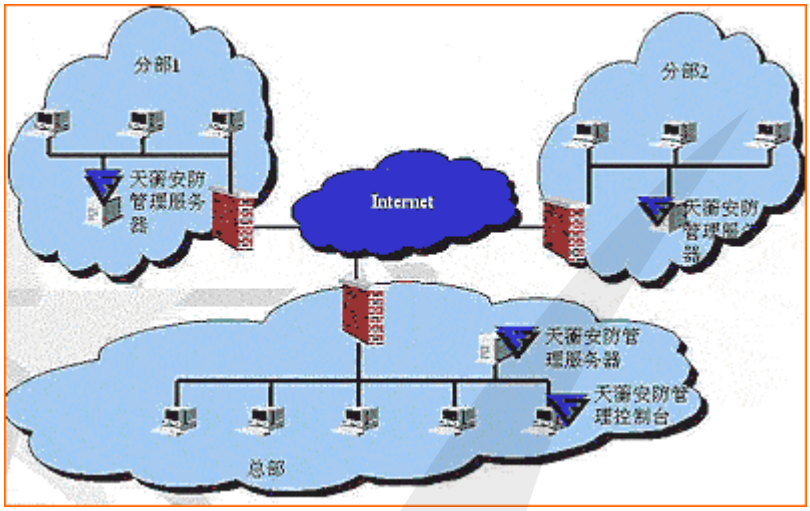
存储管理员发布的策略、软件的更新和被管理的主机发出的状态信息及警报。

管理代理（Management Agent）

用来实施管理员在被管理的主机上设置的安全策略，并为最终用户提供用户界面和其它服务。

其层次关系是管理员工作站、后台服务器和终端用户工作站。所有在管理员工作站和终端用户工作站之间的通讯都通过这个体系结构来实现。

天衢安防的策略管理器可以通过 HTTP 协议或共享目录进行通讯，因此管理员所下发的策略文件和最新的病毒定义文件可以通过广域网及国际互联网传输，实现真正的对广泛分布用户的集中管理。



世界一流的病毒检测和清除能力

天衡安防网络防病毒系统采用 Countersign 技术将多个不同的扫描引擎集合在一个产品内，这几个扫描引擎分别是：

F-Prot——最好的宏病毒检测和清除引擎，同时拥有一流的文件和引导扇区病毒检测和清除能力。

AVP————最好的多态文件病毒检测和清除引擎，一流的宏病毒检测和清除能力。

Orion——世界上第一个也是仅有的提供启发式的和模拟方式的扫描引擎，可探测出基于设备文件的变体 WIN32 病毒。

多重引擎扫描技术是唯一可跨平台使用的产品，多个内置扫描引擎可同时应用基于签名的病毒扫描器、启发式分析算法和校验和认证三种扫描技术，使之成为唯一能扫描出加密文件内病毒的防病毒产品

多重引擎扫描技术可以提供非常高的病毒清除率。所有的防病毒产品都工作在一个通用的框架（Framework）之下，并且，因为内置的多个病毒扫描引擎可以应用不同的检测技术，利用每个扫描引擎对不同种类病毒的扫描优势，使得病毒处于交叉火力之下，从而大大提高了查杀率。

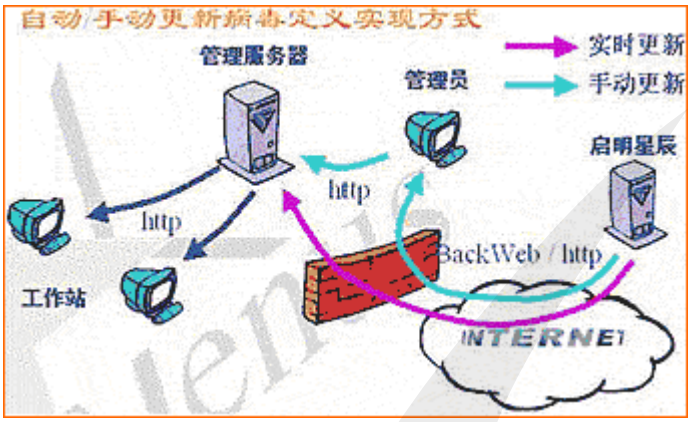
天衡安防网络防病毒系统是一个完全模块化的防病毒程序，不同的模块可以被单独维护和升级。

自动更新病毒定义文件

防病毒客户端以轮询方式自动从管理服务器获得更新，轮询时间间隔可以由管理员设定；

更新的病毒定义库可以由管理员手动放置到管理服务器上，也可以通过 BackWeb 服务器端程序自动从 Internet 接收更新。Back Web 客户端与 Back Web 服务器端以频道订阅式连接，

所有更新文件将自动从服务器端 Push 到客户端，此过程支持断点续传，同时病毒定义库的更新是以字节级增量式进行的，它使用闲置带宽，不抢占宝贵资源。通过这种方式，用户可以建立一个 100%全自动的病毒定义更新系统。



完备的病毒定义数据库

病毒定义数据库的内容是衡量防病毒产品检测和清除病毒能力的一个重要指标。天衢安防同时拥有世界五大病毒库之一的 F-Secure 公司的病毒定义库和国内完备的病毒定义数据库，使得天衢安防的病毒检测和清除能力技高一筹，无论是国际上流行的病毒还是国内流行的病毒，天衢安防都可以及时准确的将其检测和清除。

独特的邮件服务器扫描技术

天衢安防使用 Content Scanner 与邮件服务器分开查杀病毒的方式。

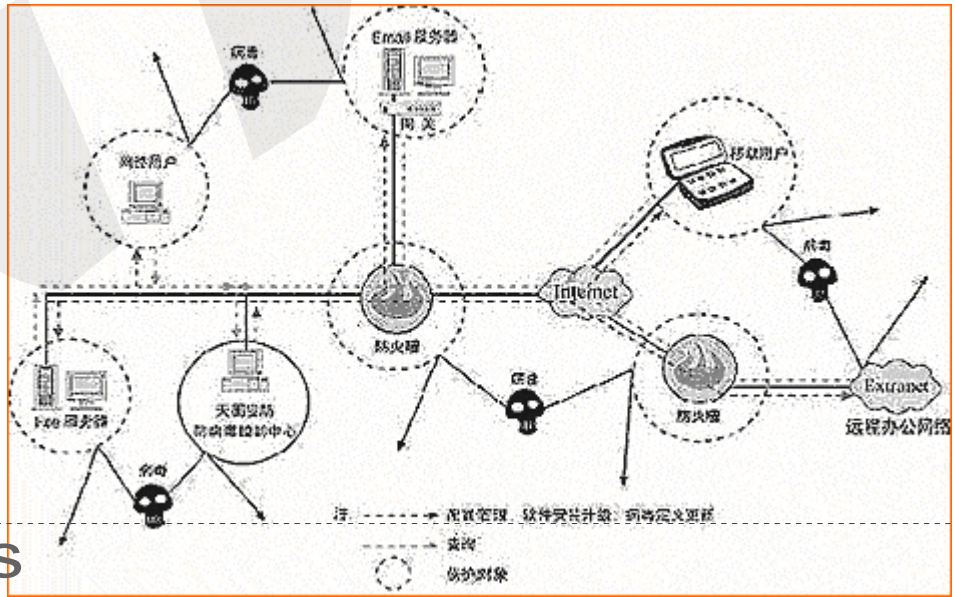
天衢安防网络防病毒系统服务器版由两部分组成：AntiVirus Agent 和 Content Scanner Server。其中 AntiVirus Agent 主要负责在服务器中向 Content Scanner Server 转发邮件或文件，Content Scanner Server 进行文件的病毒检测和清除工作，并向服务器返回结果。

具体说就是将所有要检测病毒的邮件写入天衢安防在邮件服务器中建立的数据库，通过 FNP（F-Secure network protocol）协议，将数据库内的邮件传到 CSS（Content Scanner Servers），在此处对邮件进行查杀，检测之后将邮件传到邮件服务器内。

天衢安防所建立的数据库可以被设置清理邮件的时间和次数，也可被中止扫描..如有通讯中断的情况，所有邮件会被存放在这个数据库中，并按系统设置定期试图建立连接。一旦接通，继续正常工作。特别在 Lotus notes 下，由于 Lotus Notes mail.box 的‘脆弱’性，天衢安防数据库中的邮件，可以作为 lotus notes 的备份。

这种方式可以减少在邮件查杀过程中给邮件服务器增加的额外负载，避免邮件服务器因过载而崩溃。

下图是天衢安防网络防病毒系统框架及实现功能的应用结构图。



Webkeeper 网站监测与修复系统

随着互联网络的迅猛发展，建设网站，通过建立 WEB 网站宣传形象、开展业务，已经成为政府办公，企业发展的重要手段。然而人们在享受网络带来的便捷和机遇的同时，也越来越被黑客入侵事件所困扰，确保 Web 网站的安全是亟需解决的问题。

启明星辰信息技术有限公司最新研发的网络安全产品 WebKeeper v3.0 ，结合实时触发和比较扫描的双重技术的各自优点，采用贴近操作系统内核方式的控制技术，有效保障网站数据的安全性和真实性，为您的网站提供实时自动的安全监护。

主要功能

实时阻断和自动恢复

在对网页文件、ASP 页面的控制原理上采用两种保护机制：产品即可以对被保护内容的非法操作进行实时阻断而拒绝非法修改、替换和删除，也可以通过实时监控和定期扫描的方式对已被非法操作的文件进行自动恢复。两种机制还可以结合使用，极大的增强了用户使用的灵活性和安全性。

触发式自动扫描

采用触发式扫描方式，利用文件特征码只对被修改的文件进行扫描，大大减少了对被保护文件的监控反应时间，并节省了大量的系统资源。

及时报警

对所有的非授权网页修改、删除操作做到立即发现，及时报警。

增量备份

采用增量备份方式增加备份库内容，每次修改静态页面不需要将备份库初始化，备份文件耗时非常短，占用资源少。

多用户管理

允许用户设定上传工具，系统运行期间可对保护项目添加、减少，同时能够实施多用户管理，便于多点发布合法更新网站内容，无须停止本系统。

异机备份

备份库可在异机实行，确保备份库安全。

远程控制

可以进行远端控制，也能进行本机操作，用户可根据实际情况灵活应用。

日志管理

提供完整的日志记录，易于查阅、管理，同时也可以进行合法修改的日志过滤，免除因日志记录过多造成的管理员负担过重。

安全可靠

用户如果选择不允许关机，则系统不能被强行关闭，并具备自行锁定功能，相关操作需要严格的密码认证。

使用特点

安装简便

安装程序引导，依照提示进行，无须繁琐设置。

界面友好

所有管理是基于图形界面操作，用户界面简洁、友好，网站管理员可以非常容易的根据用户手册独立操作。

配置简便

提供对整机文件系统的浏览，用鼠标点按或拖拉，即可完成配置库的设置。

资源占用

系统平时处于后台监测状态，在没有发现异常时占用系统资源很少，一旦发现异常及时阻断或恢复，并释放占用资源，对系统正常工作无不良影响。

运行环境

1、 监测端操作系统要求：

WinNT4.0/Service Pack4/IE4.0 以上；Win2000 Professional/Server/Advanced Server

监测端硬件配置要求：

Pentium 133 以上，64MB 以上内存，2GB 以上预留硬盘空间

2、控制端普通 PC 机即可

升级与更新

不定期进行版本更新，用户可从网上直接下载最新升级文件。

安星主机保护系统

1 安星单机版

系统定义

安星个人主机防护系统是对 Windows9X 环境下的资源进行保护的一个应用，用于防止黑客入侵、木马程序和重要的个人系统信息泄露的信息安全保护系统。保护范围包括系统的网络通信信息、文件访问控制、系统配置信息和防止通过 Modem 进行电话盗拨。

它以系统默认策略和用户自定策略为保护的依据，从文件、注册表、网络通信、拨号网络四个方面进行控制。这几个方面的保护相互补充，为用户的主机建立了一个安全的从里到外的防护系统。

系统主要功能

防黑客能力

结合对针对个人主机的黑客攻击方法，提供大量的经过测试检验的策略方法库，全方位多侧面的对不同应用、不同环境的个人主机系统面临的系统威胁做出反应，可以可靠保护个人 PC 系统的稳定运行和信息安全。

系统可以保护的个人主机信息系统安全威胁有：

1、网络拒绝服务攻击，如对固定端口的数据轰炸

2、非正常网络访问，如 BO、冰河一类的木马程序

3、非法修改系统配置（注册表、配置文件）

4、非法访问或替换系统或重要信息文件

文件防护

通过对文件的打开、读、写、重命名、删除进行控制，可以拒绝非法用户的访问，从而达到保护文件的作用，另外一方面，该系统还默认对保障 windows 系统正常运行的文件进行保护。

注册表防护

是保护注册表的键不被打开、创建、删除，注册表的值不被查询、读取、修改。通过这些控制可以保护一些应用的正常运行，保护一些应用不被非法用户使用，禁止非法用户应用、改变系统的资源。

拨号网络防护

主要是保护用户在拨号上网时只能拨打用户自定义的 ISP 的接入电话，保证了用户的电话不被盗拨到其它地方。如果没有设置，系统将禁止拨号上网功能。

网络通信防护

主要是禁止用户的机器被一些网络上的非法用户访问，如端口扫描、木马植入等，也可以限制该主机访问其他用户可以访问的地址。这个保护是基于 TCP/IP 协议的，在 ICMP 方面主要保护了 ping 功能，在 TCP/IP 方面保护了 IP、TCP、UDP 通信。

系统特点

安装简单，界面友好，充分考虑了不同层次的用户的用户习惯；

设置简单但又有较强的自身安全性，可确保主机管理者（产品注册用户）的利益；

即有全面的默认防护策略，又可实现用户的自定义策略设置；

支持灵活的报警方式选择，不影响用户的正常工作；

全面的多种日志查询方式，忠实记录所有安全信息

系统运行环境

系统要求 WINDOWS98 操作系统，32M，celron 400 以上 PC

2 安星网络版

网络版概述

企业级的管理不同于单机用户，企业需要对局域网内的用户进行集中管理，安星网络版是启明星辰公司在单机版的基础上开发的，对企业用户的主机防护、网络防护进行集中控制管理的安全系统。

安星企业防护系统强大的功能、简单的操作、友好的用户界面、全面的技术支持解除了您的后顾之忧，是值得信赖的信息安全产品。让安星成为您企业的守护神，安全地维护着您企业的利益！

体系结构

安星一级控制中心

安星一级级控制中心的功能主要体现在两个方面，一是监控安星二级控制中心的的运行状况，二是控

制安星客户端的运行状况；

监控二级控制中心的运行状况，获取二级控制中心的信息，这些信息包括，二级控制中心的主机 IP 地址、判断 IP 是否合法、受控状态、统计信息描述（包括该二级控制中心的扫描网段的合法、受控、非法、IP 变化主机数量）。

控制安星客户端的运行状况包括，首先下发网络通信和拨号保护策略给二级控制中心，通过二级控制中心将策略下发到安星客户端，从而达到对安星客户端的控制。其次是获取安星客户端的信息，这些信息包括主机 IP、IP 是否合法（包括合法和非法两种状态）、受控状态（包括受控、不受控、关机三种状态）、统计信息描述（客户端的网络报警和拨号报警的数量）、IP 变化情况（包括无变化和 IP 由 x 变化为 Y）。

安星二级控制中心

安星二级控制中心的功能主要体现在两个方面，一是监控安星客户端的运行，二是维护整个网络的封闭性。

监控安星客户端的运行状况，首先是检测安星客户端的状态信息，包括安星客户端是否开机，开机后是否启动了安星客户端，处于二级控制中心的控制之下，安星客户端的 IP 地址是否发生变化，变化的原地址和改变之后的地址是什么。其次是控制安星客户端，二级控制中心通过定制网络通信保护策略和拨号网络保护策略，将策略下发到安星客户端，安星客户端在控制端定制的策略的前提下运行，如果安星客户端有策略限制的操作出现，在客户端就会产生报警信息，并且向控制端上报报警信息，为系统管理员进行网络管理提供依据。

维护整个网络的封闭性，二级控制中心通过扫描所管理的网段的各类设备，从而检测出是否有非法的主机接入，从而维护整个网络的封闭性。

安星客户端

安星客户端的基本功能和安星单机版一致，其文件防护、注册表防护是由主机使用者自行定义，网络通信防护和拨号防护既可以由用户自行制定，也可以强制执行上级控制中心下发的保护策略，为了便于集中管理和整体安全防护，上级策略的优先级高于用户自定义的策略。安星客户端的报警信息日志可以上传到控制中心，做统一分析。

安星客户端即将推出 WIN 2000 Professional 版本。

系统应用环境

控制中心： 包括一级控制中心和二级控制中心

硬件：CPU：80586 (建议 Pentium 166 以上)

内存：32M（建议 64M 以上）

硬盘：2G 剩余空间

软件：Windows 9x 环境以上(包括 Windows 9x)

客户端：

硬件：CPU：80586 (建议 Pentium 166 以上)

内存：32M（建议 64M 以上）

硬盘：15M 剩余空间

软件：Windows 9x 环境

网络版主要特性

控制端、客户端分级管理一体化

一级控制中心给二级控制中心下发网络和拨号策略，二级控制中心将从一级控制中心接收的策略再下发给它所控制的所有安星客户端，从而达到安星一级控制中心对安星客户端的间接控制；二级控制中心可得到客户端反馈的概要信息和详细信息并上传至一级控制中心

支持各种标准服务及用户自定义服务

可以支持的协议标准是评价一个主机防护系统的重要指标之一。安星网络版基于 TCP/IP 协议，在 ICMP 方面主要保护了 ping 功能，在 TCP/IP 方面保护了 IP、TCP、UDP 通信。客户端在控制中心下发策略的基础之上，根据用户需要可以自定义防护策略，实现用户个性化应用。

高扩展性

二级控制中心和客户端的数量可以随时增减，而不会影响系统的正常运行。

默认策略实时防护

通过制定默认防护策略的高、中、低级别，系统分别对操作系统的系统文件、注册表、网络通讯实施安全防护。适合各个层次的用户使用。

强大的网络监控管理

监测网络中是否有主机接入，维护监控网端的封闭性

强制性的提高办公用户的安全性和办公效率。

监测用户的拨号行为,并对非授权的拨号进行阻断

监测客户端发生的和制定策略相匹配的所有操作行为

控制中心集中收集网络所有客户端报警信息，并迅速采取对应措施

安星网络版的典型应用

在某政府网络环境中，安装安星个人主机保护系统的网络版，共 240 个被保护点，客户环境：

服务器：惠普 HP LH6000 型

配置： XEON 700M*2/512M/2*18.2G/RAID 0

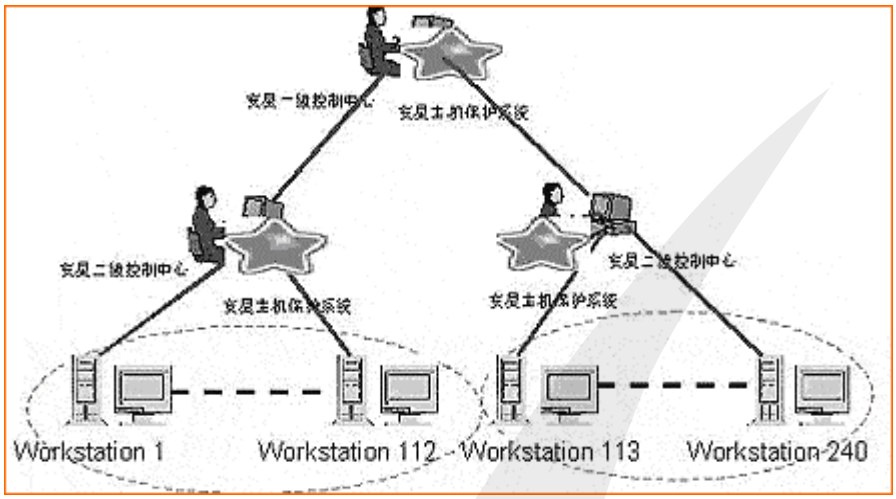
应用平台： Windows 2000 Serve

工作站：联想 奔月 2000

配置： PIII1000MHZ/128M/30G/ 17''/50X/声卡

应用平台： Windows 98se

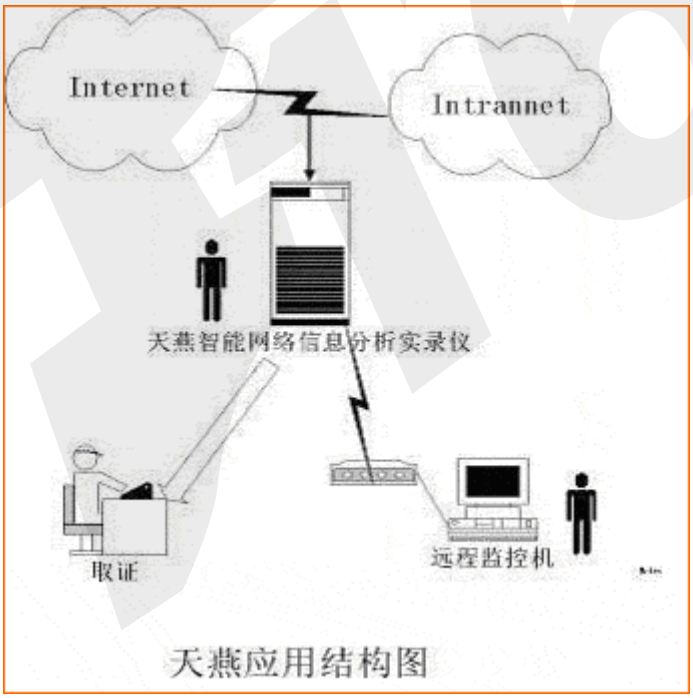
满足了对防黑客、内部文件保护、拨号网络防护和注册表的保护方面的需要，受到客户的好评。其网络拓扑结构如图：



天燕智能网络信息分析实录仪

天燕智能网络信息分析实录仪是一种放置在重要网络干线上、不间断进行网络信息分析和数据安全记录的高度集成化的大型仪器，具有高运行效率、高可靠性、高安全性，可为公安、检察、法院等机关追踪计算机犯罪提供线索和确凿证据，同时也能够为金融、证券以及电子商务网上交易安全记录重要数据信息。

天燕从硬件角度充分考虑其物理安全性，保证记录数据的真实性和高度可靠性，从软件角度实现了大流量监控、智能判别和实时记录，成为审计取证的可信赖的网络安全工具。



天燕应用结构图

硬件特点

机柜正面采用钢化玻璃，侧柜及后面板采用内开启方式，并采用智能锁或指纹锁和防盗开报警装置；

通过机柜所有部件的状态指示灯，可以方便了解各部件运行状况；

金属外壳显示器实时显示报警信息，与主机显卡连接的数据线装有信号抗干扰器，整体具有防外部电磁干扰和内部电磁泄露功能；

采用实时刻录的光盘记录仪，方便记录网络上的数据，并实现真正意义上的海量存储和数据的不可更改和擦除；

双网卡结构，保证内外网物理上隔开；

主机具有从远程监控开启机器面板、控制主机内硬盘温度、排风扇流量的传感器，并可远程开关主机电源；

主机机箱内敷特殊防电磁泄露材料；

高精度的温度、湿度控制器，可监控整个机柜内温度和湿度，并自动调节机柜内温度和湿度；

良好的自动除尘系统，无须打开机柜，实现定期自动过滤除尘；

采用安全加密调制解调器，实现远程控制传输；

提供多功能工具箱，内放多种常用维修工具，存放防静电装置（手套、鞋套），并有一部电话，保证维修时人员无须离开机柜保持与外联系；

长效延时纯在线式的 UPS，其延时时间长，更能稳定工作；

具有防雷电设施，防止实录仪被自然雷电所损坏而造成重要数据丢失；

所有部件遭非法移动都会启动报警装置。

软件功能

能够全面监控网络中信息流量，可适应大流量的网络数据传输；

可智能的判断出网络中所有合法和非法操作，提供报警功能，便于管理员及时发现并采取应对措施；

可显示其数据报文的来源和不可更改的时间项标记，为调查取证提供可信证据；

对所有非法操作和可疑网络行为的数据实时记录，准确分析，必要时可形成人性化的报表输出；

具有严格的身份认证，确保只有合法管理员才能拥有唯一的管理权限；

支持远程安全监控，并切断所有黑客可能侵入本机的途径；

能够较好的支持硬件设备的性能特点和技术要求；

对网络数据传输无不良影响；

C-SAS 客户化安全保障服务

1 安全理念

安全保障

随着互联网络的普及发展，政治、经济、军事、文化、科技和教育等社会各领域面临的威胁风险日益

增多，对安全的需求越来越迫切，国家政府对安全越来越重视，由此诞生了一门崭新的学科——网络安全工程学。

网络安全的本质已趋向于网络信息的安全保障，投资与行动更加理性化、简单化，强调的是及时性、普及性、健壮性和完善性。安全程度不能用绝对的数字来表示，而应在模糊逻辑基础之上尽可能地去量化。

动态安全过程

由于黑客攻击手法层出不穷、千奇百怪、日新月异，迫使安全防御技术必须同步跟进，否则有时前期的安全投资不再有效，造成巨额的浪费。因此在准备实施一个安全项目工程，构筑自身的防御体系机制时，我们认为：网络安全不能仅仅依赖于众多安全产品的作用，也不能仅仅只停留在“三分技术，七分管理”的概念上，安全不应该作为一个目标去看待，而应该作为一个过程去考虑、设计、实现、执行。通过不断完善的管理行为，形成一个动态的安全过程。

安全动态防御体系

用户目前接受的安全策略建议普遍存在着“以偏盖全”的现象，它们过分强调了某个方面的重要性，而忽略了安全构件（产品）之间的关系。因此在客户化的、可操作的安全策略基础上，需要构建一个具有全局观的、多层次的、组件化的安全防御体系。它应涉及网络边界、网络基础、核心业务和桌面等多个层面，涵盖路由器、交换机、防火墙、接入服务器、数据库、操作系统、DNS、WWW、MAIL 及其它应用系统。

静态的安全产品不可能解决动态的安全问题，应该使之客户化、可定义、可管理。无论静态或动态（可管理）安全产品，简单的叠加并不是有效的防御措施，应该要求安全产品构件之间能够相互联动，以便实现安全资源的集中管理、统一审计、信息共享。

目前黑客攻击的方式具有高技巧性、分散性、随机性和局部持续性的特点，因此即使是多层面的安全防御体系，如果是静态的，也无法抵御来自外部和内部的攻击，只有将众多的攻击手法进行搜集、归类、分析、消化、综合，将其体系化，才有可能使防御系统与之相匹配、相耦合，以自动适应攻击的变化，从而形成动态的安全防御体系。

客户化安全策略

客观来讲不存在一个 TOTAL SECURITY SOLUTION（完全的安全解决方案），来解决所有的安全问题。保障安全的首要任务应该是编写安全策略（SECURITY POLICY），即提供一套理性的、客户化的、可操作的、较全面的安全策略。 安全策略是一切安全行动（包括管理组织、管理制度、培训、操作、实施、监控、响应等）的指南。

安全策略的重点就是明确保护对象、保护原因、保护方法和实施保护的次序，明确安全责任，及相对应的处理措施。只有拥有了一个良好的安全策略，才有可能使业务运转效率、网络性能指标、安全保护等级和安全投资达到理想的均衡状态。

安全人（管理与培训）

网络安全保护的对象由人创建、由人在用、由人在管。而网络攻击的发起者也是人，攻击目的来源于他的思想意识。所以网络安全的核心必然是人。对攻击者进行安全法律法规教育，对执行者进行安全技能培训，这项工作应贯穿整个安全过程。

与安全技术相比，涉及人的安全管理非常重要，应包括安全策略管理、安全组织规范、资产分类与控制、人员安全管理措施、物理与环境安全保障、通讯与操作管理程序、访问控制要求、系统开发与维护规程、业务连续性管理办法和法律法规一致性规定等内容。

2 C-SAS 诠释

启明星辰信息技术有限公司基于全新的安全理念，提出并实施客户化安全保障服务（Customer Security Assurance Service）。

客户化，即网络现状分析客户化、安全需求分析客户化、安全策略设计客户化、防御体系构建客户化、管理客户化、培训客户化、响应客户化。　安全保障，即指人（法律法规教育、技能培训、物理安全、人事安全、系统安全管理），依靠技术（保障框架、安全标准、评估、认证、产品采购），执行安全操作（风险评估、实时监控、入侵检测、报警响应、灾难恢复、审核审计），来保障网络信息安全。

服务是可管理的产品，更是一项系统工程。做好服务，需要拥有理论研究专家（设计策略、体系模型、等级保护、专业培训、管理制度）；能够提供自开发的系列安全产品，又能够提供客户化产品定制；具备攻防实验实力（动态响应）；拥有由攻防、开发队伍中培育出的技术支持人员（构建安全防御体系）；拥有系统集成队伍（工程实施与维护）。

C-SAS 服务体系

总体框架

C-SAS 星系图

安全人：

网络安全的核心就是人，包括使用者、攻击者、防御者、管理者，所有的安全策略、安全管理、安全培训、风险评估、方案设计、防御体系和动态响应都在围绕着安全人运转。

安全理念：

安全理念是人的思想在安全领域中的体现，是服务提供者和服务使用者达成共识的根本基础。理念是否一致直接影响着策略是否切合实际，策略导向性是否正确。

安全策略：

安全策略是一切安全行动（包括管理组织、管理制度、培训、操作、实施、监控、响应等）的指南。

安全策略首先落实到行动上就是安全组织管理。

安全管理：

涉及众多方面的安全管理（包括策略、组织、资产、人员、环境、操作、控制、维护、规定等）非常重要。要有效地持续性管理，需要做好不同阶段的各种教育、培训。

基于角色的安全培训：

针对于安全过程中不同的角色进行相应的培训，包括安全意识的培养、法律法规的教育，安全技能的培训。培训应贯穿整个安全服务过程。

安全服务：

服务工程主要包含安全策略、风险评估、体系设计、实施防御和动态响应，能够体现次序性、阶段性和循环性。

服务组件总表

组件类别	编号	件名称	目标
C-SAS 安全策略	C-SAS.SP.01	安全策略纲要	简要描述保护对象、面临威胁、防护措施、责任制度、后果处理。
	C-SAS.SP.02	网络现状分析	重点分析网络性能、业务特点，确定安全需求基础。
	C-SAS.SP.03	网络安全需求分析	分析当前安全状态，确定安全设计总则。
	C-SAS.SP.04	威胁风险评估	分析攻击威胁，确定安全风险，建议安全实施策略。
	C-SAS.SP.05	安全策略设计	确定安全行动（包括管理组织、管理制度、培训、操作、实施、监控、响应等）的指南。
C-SAS 安全管理制度	C-SAS.SM.01	安全管理基本要求	确定安全的组织、人员、制度、业务流程。
	C-SAS.SM.02	安全管理详细规范	制定策略、组织、资产、人员、环境、操作、控制、维护、业务、规定等详细规范。
C-SAS 安全防御体系	C-SAS.SD.01	网络组件加固	对边界组件（路由器、交换机、防火墙）、基础组件（操作系统、数据库）、应用组件（WWW、DNS、MAIL）等加固。
	C-SAS.SD.02	渗透性测试	从边界向网络内部，分层进行无损探测及渗透。
	C-SAS.SD.03	安全构件（产品）选型	提供安全产品的选型、测试、布设方案、培训与服务。
	C-SAS.SD.04	安全监控	对指定系统进行日常监控、记录日志、审计分析。
	C-SAS.SD.05	网页自动恢复	监控关键网页、阻断非法访问、自动进行完整性检查并恢复。
C-SAS 动态安全响应	C-SAS.SR.01	定期漏洞扫描	对边界组件、基础组件、应用系统进行漏洞扫描，给出分析报告及安全建议。
	C-SAS.SR.02	最新漏洞修补	及时发布最新漏洞疫情、修补建议及措施。
	C-SAS.SR.03	紧急事件响应	快速响应入侵事件，修复系统漏洞，加固组件，恢复数据，追踪入侵。
C-SAS 网络防病毒服务	C-SAS.AV.01	现场网络杀毒	全方位、跨平台、多层次、广域网的网络杀毒。
	C-SAS.AV.02	客户杀毒服务外包	面向大型客户，提供全面网络杀毒外包服务。
C-SAS 网络安全培训	C-SAS.ST.01	网络安全基础	法律法规，网络安全基础
	C-SAS.ST.02	网络安全策略	风险分析与管理，安全策略设计
	C-SAS.ST.03	网络安全工程和实施	网络安全结构设计，安全机制的测评系统，信息系统安全工程
	C-SAS.ST.04	网络安全技术	信息安全技术，公用密钥基础设施PKI和CA，访问控制技术，防火墙技术，入侵检测技术，漏洞扫描技术，网络防病毒技术，数据库系统安全，网络攻击方法与防御。
	C-SAS.ST.05	网络安全配置管理	UNIX安全配置与管理，NT安全配置与管理，网络安全管理，网络安全资源管理
	C-SAS.ST.06	网络安全实践	漏洞扫描试验，入侵攻击试验，入侵检测与预警试验