V3 系列

网络防病毒系统

安博士有限公司

2004

目录

1 项目介绍 4

1.1 项目介绍 4
1.2 安博士有限公司介绍 4
1.3 项目需求 6
1.4 安博士有限公司系列产品介绍 7

2 V3系列网络防病毒系统介绍 8

2.1 安博士策略中心软件（AhnLab Policy Center 2.0）的介绍 9
2.2 主要功能及特点 9
2.2.1 统一的策略管理 9
2.2.2 登录及状态标示功能 11
2.2.3 应用安全命令 12
2.2.4 关于安全管理的其他附加功能 12
2.2.5 便利的统计及报表生成工具 13
2.3 V3系列网络防病毒系统客户端/服务器端介绍 13
2.4 V3系列网络防病毒系主要特点 14
2.4.1 彻底阻断通过邮件流入的病毒 14
2.4.2 彻底阻断通过互联网流入的病毒 14
2.4.3 内置病毒监控、自动修复功能 14
2.4.4 用户操作权限管理 15
2.4.5 对病毒的确认及安全的修复选项 15
2.4.6 高效率防疫・管理的各种附加功能 15
2.4.7 环境设置向导 15
2.4.8 以迅速的升级维护系统安全 15
2.4.9 内置强有力的WARP引擎 16

3 V3系列网络防病毒系统的网络结构及组成 16

3.1 AhnLab Policy Center 2.0的结构 16
3.1.1 管理对象系统构成要素 17
3.1.2 管理员系统的构成要素 18
3.1.3 管理服务器系统构成要素 18
3.2 产品的结构特征 19

4 V3群件服务器防护系统介绍 21

4.1 V3NetGroup for Lotus Notes介绍 21
4.1.1 主要功能介绍 21
4.1.2 产品特点 22
4.2 V3NetGroup for MS Exchange介绍 25
4.2.1 主要功能介绍 25
4.2.2 特点介绍 26

5 V3网关邮件防病毒系统介绍（SMTP协议） 28

5.1 V3GateBlock产品功能和特点介绍 28

6 安博士在线安全产品介绍 29

6.1 网络在线安全现状 29
6.2 MyV3 在线杀毒 30
6.2.1 MyV3的基本概念： 30
6.2.2 MyV3的主要功能： 30
6.2.3 MyV3的系统特征 31
6.2.4 MyV3的优点 31
7 服务与支持 32
7.1 用户支持服务 32
7.2 技术支持与服务 32
8 附录 32
8.1 国内外主要客户名录 32

1 项目介绍

随着电脑的普及，几乎所有的电脑用户都已知道“计算机病毒”这一名词。对于大多数计算机用户来说，谈到“计算机病毒”似乎觉得它深不可测，无法琢磨。而对于企业用户，由于办公自动化及电子商务的逐步深入的应用，企业对于计算机网络的依赖越来越强。这使得企业的办公效率进一步加快，给企业带来了巨大的效益。但是，同时计算机病毒及黑客也给企业带来了极大的风险。试想如果由于病毒或黑客的袭击，使得整个企业办公网络瘫痪、数据库无法进行查询或重要数据丢失、重要文件无法使用、计算机通信无法进行甚至重要客户资料被黑客窃取等情况发生，将给企业带来多大的损失。所以企业网络的防病毒及黑客更是比单机防病毒更为重要。此反病毒系统方案，是针对 V3 系列的网络系统特别提出和设计的。

1.1 项目介绍

1.2 安博士有限公司介绍

安博士有限公司成立于 1995 年，作为亚洲地区最大的反病毒及网络安全产品提供厂商，自成立以来相继推出了防病毒、CA 认证、安全咨询、安全监控管理、安全 ASP 等综合安全解决方案。并通过开展各种网络犯罪预防活动，致力于信息交流的安全及发展。

V3 系列防病毒产品是一个及 Windows、Unix、Linux、NetWare 多种网络操作系统为一体的，功能强大的新一代网络防病毒产品。V3 系列产品包括保护您的 Windows 系列产品：Windows 2000/NT Server、Windows 95/98、Windows NT Workstation、Windows 3.X、DOS 工作站，同时还提供对 Lotus Notes 和 Microsoft Exchange 群件系统的防护功能以及防护 Internet 网关的保护。V3 同样可以适用于 Novell NetWare、Unix、Linux、Sun Solaris 操作系统。V3 系列产品提供无与伦比的功能为您的企业网提供强大的防护。

V3 系列软件获得多家权威计算机安全机构的认证与推荐，其中包括中国公安部检验中心的认证及销售许可，微软公司以及亚洲反病毒协会等多项奖项。

自 1995 年成为韩国首家从事杀毒软件开发的企业，V3 系列有限公司目前已经成为代表韩国最早、技术力量最高的安全软件开发商，始终坚守着“从 PC 防护到互联网安全”的公司宗旨，致力于互联网综合解决方案的开发与海外市场的开拓。具有世界上最快、最准确的病毒查杀功能的防病毒综合解决方案 ‘V3’，彻底保护、管理网络及相连 PC 信息的‘EnDe’， 为了制订最佳安全解决方案而提供的 ‘Consulting 服务’，可在互联网方便使用的‘安全在线服务’— 安博士有限公司将通过上述世界一流技术的综合安全服务，完善地保护用户的虚拟环境。为了虚拟空间的安全 信息化时代最切实的安全装置‘安博士有限公司’与您同在。

主要价值：

— 通过不懈的努力提高自身

— 自尊、自强、自信地致力于公司发展

— 坚持诚实进取、诚信经营

公司目标：

— 通过不懈的探索和发展贡献于社会

— 力争位居全球安全解决方案提供商的前 10 位

主要提供产品：

病毒防御的全套解决方案:

- 通过安全咨询，AhnLab 为企业提供客户化、配套的反病毒服务
- 在技术性和可靠性为主的企业计算化环境中，V3 的反病毒服务被广泛应用
- 内置 V3 引擎可以 100%对感染文件进行恢复
- 每周可将引擎升级到最新版
- 通过互联网可自动进行智能升级
- 通过中央管理工具可对 V3 家族产品进行集中管理
- 根据报告，我们在 24 小时内分析并提供治疗引擎
- 在网络环境的设置中根据病毒分析报告不断更新和完善病毒防御服务

VBS(阻断病毒服务):

- 构建自动监视病毒的系统

在线的方式进行病毒保护:

- 无需安装杀毒软件，只要登陆互联网就可诊断/治疗病毒

在线的个人电脑防火墙:

- 封锁所有 Backdoor Hacking 工具 (Back orifice, School Bus 等)的入侵来源，以防止个人信息 (ID/口令/身份证号/银行帐号/卡号) 的泄露
- 防止由病毒引起的计算机感染

在线密码保护：

- 利用自身认证功能判断 KeyLogger
- 防止黑客对计算机的入侵

在线游戏的安全保护：

- 监视和防止游戏外挂的使用

1.3 项目需求

随着政府上网工程的不断普及，各企事业单位都相继建立了基于各单位的互联网络系统，然而通过使用互联网而带来了通信环境的急剧变化的同时，也带来了黑客、病毒、系统的非法入侵等各种副面作用。因此，多种多样的个人安全软件得以开发出来以实现对计算机系统的保护。使您的系统免受病毒入侵的 V3 Virusblock/V3 Virusblock for Windows Server 等反病毒软件软件，已经得到广泛的使用。

但是，诸多个人用安全软件产品，如果得不到使用者的不断关注和正确使用，就会成为无用之物而被弃之一旁。并且安全管理人员如果在使用了安全软件之后，便认为完事大吉而错误地认为个人计算机的安全已经很周密了的话，在真正发生了安全事故时便会束手无策而陷入被动的困境之中。

企业的安全管理员为了实现整体的安全管理，可能在每台个人计算机上安装了反病毒程序、个人防火墙或入侵检测系统等各种形式的安全措施，但是由于人员所限，很难对所安装的措施进行有效而持续的管理。

- 个人安全管理的薄弱环节

安装于个人计算机的 PC 安全产品并不能自动地应对一切安全威胁。例如，安装于个人计算机的反病毒软件应该不断地对检索引擎进行更新以保持最新版本，通过周期性地对病毒进行检索而阻止病毒的侵入，并通过对侵入的病毒进行统计等程序形式，从而对系统实现

连续的管理。 但是大多数的个人计算机用户在很多情况下，由于对病毒认识不足，在安装了软件之后便置之不理了。并且即使在公司内部的所有计算机中都安装了个人用防火墙，也难以对所有个人用户设定适合公司内部安全策略的网络设置。

- 多种安全管理指向

如今计算机入侵的种类显得更加复杂，威胁的形式也更加多样。各种安全产品为了应对这些入侵，提供更加多的功能，而使得复杂性不断加大。因此，对为实现对这些复杂而多样的安全产品进行管理，就需要增加资源投入，从而增加了全部的所需费用。

- 建立整个公司的安全策略的必要性

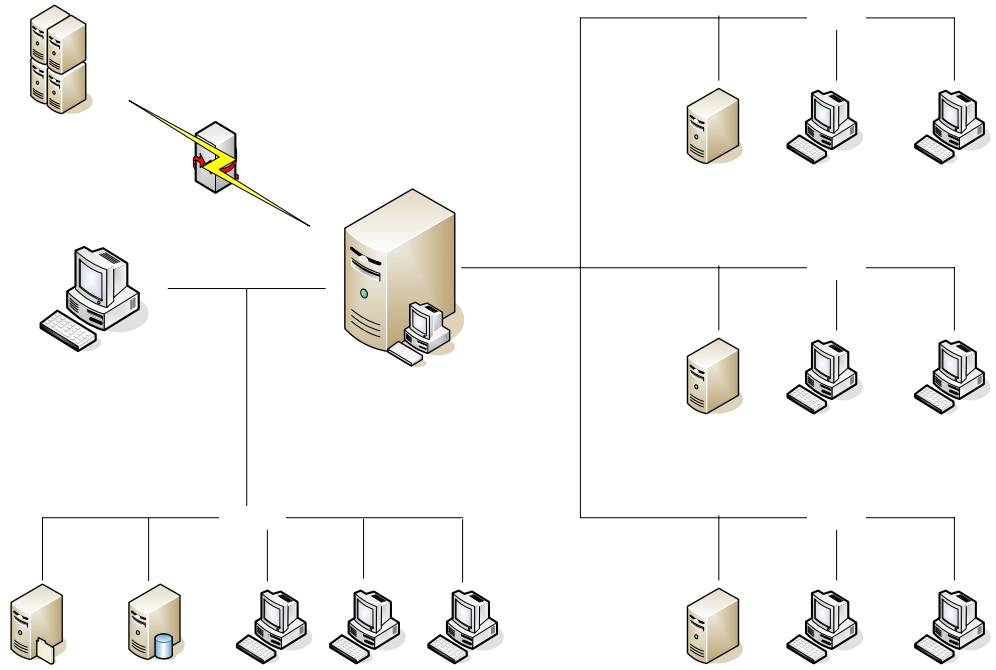
公司内部的个人计算机安全，不仅是只影响个人的计算机环境，因为面对日益复杂而肆虐的安全威胁，即使只有一两台计算机暴露出薄弱环节，也有可能很容易地导致公司内部全部计算机网络出现瘫痪。所以有必要对安装于个人桌面的各种计算机安全产品和该产品所需的定期的操作，以及它们所形成的安全记录等实现中央控制。

- 对安全威胁迅速进行处理

在公司内部发现恶性信号扩散或黑客试图进入时，为了防止威胁的扩散，需要所有的个人计算机用户统一采取行动。但是在实际情况中这是无法实现的事情。因此在发生安全事故时，在没有个人用户介入的情况下，需要由安全管理员统一进行有条不紊的安全策略操作。

安全管理负责人只要在中央服务器中安装一个安全策略，通过各个安全产品与用户计算机的有机配合及定义好的程序，以维持运行安全策略，这就是安博士策略管理中心软件（AhnLab Policy Center 2.0）的统一安全措施方案。

1.4 安博士有限公司系列产品介绍



2

V3 系列网络防病毒系统介绍

AhnLab Update Server

V3 系列网络防病毒系统是由安博士有限公司推出的企业级网络防病毒软件。不同于其它防病毒软件的是：它是一款完全按照大型网络结构和企业复杂计算机环境需求设计的新一代网络防病毒系统。因此除具有对病毒良好的查杀效果外，整个系统的结构伸缩性强，管理功能强大，完全适合各种规模的企业部署。

此网络防病毒系统是新一代的网络防病毒产品，对于目前越来越广泛传播的网络病毒有多重的防护能力，可确保企业内部网络不受病毒侵扰。

V3 系列网络防病毒系统产品由以下几部分组成：

- 安博士策略中心（AhnLab Policy Center 2.0）
- 安博士防病毒服务器端（V3 VirusBlock）
- 安博士防病毒客户端（V3 VirusBlock for Windows Server）

Policy Admin

V3 系列网络防病毒系统，可对如下平台提供全面病毒防护：

- Windows 95/98/Me
- Windos NT Workstation
- Windows 2000 Professional

- WindowsXP Home/Professional
- Windows NT/2000/2003 Server

V3 系列网络防病毒系统的核心是由策略中心、防病毒客户端、防病毒服务器端共同组成的一个全面的针对 windows 平台用户的网络防病毒管理应用系统，防病毒客户端和服务器端由策略中心统一进行分发安装、统一配置和管理，这三者的结合保证了用户防病毒策略的集中实施和控制。

2.1 安博士策略中心软件（AhnLab Policy Center 2.0）的介绍

AhnLab Policy Center 2.0 软件是安博士有限公司管理安全产品系列的中央管理程序。即把设置在企业内部使用的多台计算机中的各种安全产品合而为一，根据统一的安全策略实现中央集中管理的安全管理策略。如果您使用了 AhnLab Policy Center 2.0 软件，就可以利用设置在公司内部的各种安全产品，切实地实现中央控制。并且其使用记录会统一保存于同一保存场所，并可以生成整个公司的报告书。

AhnLab Policy Center 2.0 软件是安博士有限公司对基于视窗系统的反病毒程序 V3 Virusblock/V3 Virusblock for Windows Server 和 PC 综合安全解决方案 AhnLab Client Security 1.0 软件进行中央综合管理的产品。

AhnLab Policy Center 2.0 软件具备企业内部策略管理功能、登录及状态显示功能、应急安全命令功能，以及附加功能等四种功能。

2.2 主要功能及特点

AhnLab Policy Center 2.0 作为管理个人计算机反病毒软件的产品，具有以下功能上的特征：

2.2.1 统一的策略管理

AhnLab Policy Center 2.0 是安博士有限公司所提供的软件，它通过中央服务器，对基于 Windows 系统的反病毒程序进行管理。

如果对产品组成再进行分类的话，可以细分为 V3 Virusblock, V3 Virusblock for

Windows Server 对这总共两个产品由中央服务器统一进行控制并传递主要命令。

虽然由于各个安全产品的不同其特性和使用方法也存在差异，但是如果使用了 AhnLab Policy Center 2.0 软件，在一个管理界面上通过其中的统一界面设定各种安全产品，就可以设置网络系统的安全管理策略并加以应用。

- 中央策略的统一适用功能*

企业内部安装的个人用安全产品，由于只是安装于个人用计算机，因此难于确认是否按照企业内部的规定恰当地加以使用。在 AhnLab Policy Center 2.0 软件的管理员界面中，可以对注册的所有计算机的状态和安全环境等信息一目了然地加以掌握。并且对于注册的计算机还提供了一个同时应用统一策略的、易于操作的界面。

- 安全管理产品的策略管理功能

在 AhnLab Policy Center 2.0 管理员界面上，分别对安博士有限公司的各个产品根据其产品特点提供了程序设定界面。

- 管理产品的自动配置及安装功能

AhnLab Policy Center 2.0 软件，对安装了管理代理程序的计算机提供了可以自动下载并安装安全产品的自动配置功能。借助这一功能，就可以使用户免去了一一安装安全产品的负担。并且在用户任意删除安全产品时，也可以进行重新安装，以避免出现安全方面的漏洞。

- 充分的安全策略管理功能

由于公司内部的计算机环境是多种多样的，由此而引发的安全威胁也呈现出多样性。所以为了应对这一情况，所需的安全策略也可能根据环境的不同而有所差异。也就是说，根据组织系统图表的不同，按照集团和职级，或相关部门的不同而希望实现管理的安全产品及安全策略也会在具体内容上有所差别。

为此，在 AhnLab Policy Center 2.0 软件中，对希望应用于个别或特定集团的客户，可以实现对安全产品的策略设定值进行随意的形成、修改和删除。

- 企业内部安全策略的保持

在一般情况下，安装于个人用计算机的安全软件，其安全策略即使由管理员一次性地予以设定，也有可能由于用户的原因而对该设定进行修改或变更。

在 AhnLab Policy Center 2.0 软件中，通过对中央服务器的策略进行周期性地重新应用，而实现中央服务器策略和安装于用户计算机的各种安全产品的设定的统一保持。因此可以在用户任意不适当的使用而使系统产生安全威胁时，对系统提供保护。

2.2.2 登录及状态标示功能

如果使用了 AhnLab Policy Center 2.0 产品，就可以用户计算机中产生的有关安全状态一目了然地进行掌握。例如，在 AhnLab Policy Center 2.0 的管理员界面上显示对 V3 Virusblock/V3 Virusblock for Windows Server 的实时监控是否开启的策略等根据组群或个人加以显示，因而可以轻易地掌握内部内部不符合安全策略而处于危险状态的计算机，并能迅速地采取相应的对策。

- 中央集中式的登录管理

安装于各个用户计算机的安全产品的运行记录，在保存于 AhnLab Policy Center 2.0 服务器以后，可以在管理员界面上以适当的形式显示出来。并且所保存的登录，可以对用户的详细信息及其他系统信息进行整理，从而生成各种统计及报告。

- 多种多样的报告书模板和统计功能

AhnLab Policy Center 2.0 软件可以将存贮于数据库中的各种有关安全的记录挑选出来以生成报告书。如果想使用事先定义的报告书，只需单击几下，就可以生成所想得到的主要报告书。尤其是利用统计报告书，就可以一目了然地了解到按时钟顺序排列的整个安全管理状况。

- 便利的用户定义报告书

AhnLab Policy Center 2.0 软件中虽然以多个模板形式提供了多种形态的报告书，但是根据企业的不同需要，也有可能存在不适合的需要报告的项目。为了解决这一问题，在 AhnLab Policy Center 2.0 软件中,用户可以直接选择所要求的报告书字段以生成报告书。

- 服务器和代理程序的实时监控

设置于各 PC 的代理程序向中央管理服务器实时地发送安全信息登录及事件。

如果使用 AhnLab Policy Center 2.0 软件的监视器中心功能，通过管理人员界面，就可以实现对目前中央服务器和个人用户代理程序的主要行为及状态信息进行实时监控。尤其是在病毒警报窗口中实时地对病毒发生状况进行报告，管理员可以及时采取安全应对措施。

- 策略适用状态标志

AhnLab Policy Center 2.0 软件对由中央管理服务器确定的安全策略，设计为可以

一直维持到用户的个人计算机。但是由于计算机长期关闭，或用户计算机的代理程序长期关闭，以及对个人计算机进行格式化等各种原因，也有可能出现策略无法适用的状态。AhnLab Policy Center 2.0 软件为了使这些难以对其进行管理的用户易于掌握相关状态，设计了用户界面。在管理员界面中，将各个个人计算机的策略适用状态以图标的形式显示出来。通过这一方式，管理员可以很容易地了解到哪一台计算机在安全方面处于薄弱状态，并且通过对相关的个人计算机进行检查，就可以消除企业内部在安全方面存在的薄弱环节。

2.2.3 应用安全命令

- 病毒应急对应措施

AhnLab Policy Center 2.0 软件对急速扩散的计算机病毒具有紧急应对功能。在发生急剧扩散的病毒的情况下，首先应该迅速地对引擎进行更新，为启动实时监视功能，有必要对所有的计算机再次进行检查。并且应该通过对所有个人计算机进行及时的病毒检查，并同时对企业内存在的病毒进行杀毒，以避免出现再次感染的危险。通过 AhnLab Policy Center 2.0 的便利的管理人员界面所提供的界面，只需单击鼠标，上面所列举的一系列应急病毒处理命令便可以下达到企业内部所有的计算机。

- 网络控制功能

AhnLab Policy Center2.0 软件在判定蠕虫病毒正在通过网络传播或出现黑客威胁时，将立即通过客户端软件的相关功能的控制，阻止共享文件夹的使用，以迅速应对网络安全的威胁。

2.2.4 关于安全管理的其他附加功能

- 通知事项的发送

企业内部的管理员需要经常向企业内部的个人计算机用户转达关于安全软件的使用的各种通知事项。如果使用 AhnLab Policy Center 2.0 的附加功能之一的通知事项管理功能，就可以实现向组群或个人传达通知事项。

- 软件/硬件的信息提供

AhnLab Policy Center 2.0 软件中提供了安装于管理对象个人计算机的各种软件的种类和软件种类的相关信息。这样就可以监视企业内部计算机所禁的软件或了解硬件的变更

事项。

- 远距离个人计算机的中央控制

当管理对象计算机出现异常或需要对使用方法进行说明时，在管理员界面中实现相关计算机的直接连接，从而可以实施远距离运行。无论是使用远距离计算机管理功能还是在得到用户许可后而使用，都可以实现有关远距离管理的选择性应用，以使企业对远距离管理的策略得以正确地应用。

2.2.5 便利的统计及报表生成工具

如果利用 AhnLab Policy Center 2.0 软件的报告中心，就可以生成发生在企业内部的所有病毒的有关统计及报表。对于汇聚到中央服务器数据库内的病毒的相关记录信息，管理人员可以根据群组、使用者、日期及病毒的不同，按照所希望得到的形式轻而易举地获取相关统计资料，并且可以将这些相关资料以电子表格或 HTML 的形式显示或进行编辑。

2.3 V3 系列网络防病毒系统客户端/服务器端介绍

V3 Virusblock 和 V3 Virusblock for Windows Server 是安博士有限公司所开发的应用于 Windows 9X/Me/2000 Professional/XP®的最新杀毒程序。V3 Virusblock 是用于委托程序的产品， V3 Virusblock for Windows Server 是应用于 Windows Server 的杀毒软件。V3 Virusblock 和 V3 Virusblock for Windows Server 不仅是国内外众多产品中可以提供最快速而强有力的反病毒功能的产品，而且可以对从因特网上收到的各种数据和文件是否感染了病毒进行监视、查毒和杀毒。安博士有限公司的独自反病毒引擎，不仅几乎没有误诊的可能性，而且在对被感染的文件进行杀毒时提供了出众的文件恢复功能。

- 完全阻止病毒通过邮件入侵

在 V3 Virusblock/V3 Virusblock for Windows Server 中，对依靠 POP3 传送的邮件和 Outlook 邮件夹进行实时的监控并支持人工检查。对进入 Outlook Express 或 Netscape Mail 程序的 POP3 的邮件，可以在用户接收前对是否感染了病毒进行检查。并且为 MS Outlook 提供了即插型 V3 Virusblock/V3 Virusblock for Windows Server 检查功能，即使不另外运行 V3 Virusblock/V3 Virusblock for Windows Server ，也可以对通过 MS Outlook 的邮件及邮件夹进行监视、查毒及杀毒。

- 完全阻止病毒通过因特网入侵

因特网的监视、查毒及杀毒功能，在执行系统监视功能的同时，对通过因特网传输进来的数据是否感染了病毒进行监视，在发现病毒时提供了完全的查毒和杀毒功能。

- 内置了病毒监视功能

由于采用了智能型病毒监视系统，如果在操作过程中发现了病毒，可以在系统方面阻止病毒的活动。系统监视功能尤其是在从来源上封锁病毒入侵方面具有特别出众的功能，而且这一重要功能几乎不会对系统的运行速度造成影响。

- 在发现病毒时提供准确而安全的杀毒选项

根据检查结果如果确认感染了病毒，将立即自动进行杀毒，当然根据杀毒的结果提供了安全的应对措施。也就是说，根据用户的选择选项，在准备杀毒之前为预防万一，避免文件被损坏，而将原文件保存于另外一个备份文件夹中。在万一出现无法对文件进行杀毒的情况下，系统将自动进行删除以防止病毒的继续扩散，在删除文件之前将其保存于备份文件夹中以等最后处理。另一方面可以事先确认系统是否访问了软盘，以及在 Windows 关闭时是否感染了引导病毒，从而可以完全阻止引导病毒的入侵。

2.4 V3 系列网络防病毒系主要特点

2.4.1 彻底阻断通过邮件流入的病毒

V3 系列网络防病毒系客户端提供了通过针对 POP3 邮件和 Outlook 信箱的实时监控及本地扫描功能，可以在用户收到通过 Outlook Express 或 Netscape Mail 进入的邮件之前扫描是否有病毒感染。并且在 MS Outlook 上嵌入插件程序，即使不启动 V3 系列客户端主程序也可以监控，诊断，修复通过 MS Outlook 进入的邮件。

2.4.2 彻底阻断通过互联网流入的病毒

互联网监控、扫描、修复功能与系统监控功能相结合,监控从互联网进入的文件是否被病毒感染，一旦发现病毒则及时彻底查/杀病毒。并具有阻断通过互联网下载的具有特定扩展名文件的功能。

2.4.3 内置病毒监控、自动修复功能

采用智能病毒监控（修复）系统。在系统运行中，若发现病毒，APC 将立即阻断病

毒在系统中的活动，并及时自动修复被感染文件。系统监控功能不仅在防止病毒方面具有卓越性能，而且对系统性能几乎没有影响。

2.4.4 用户操作权限管理

APC 中有些特定操作可以通过安全功能来进行保护。例如对于结束系统监控，主程序删除等操作只有通过安全认证的用户才能执行。安全认证在 APC 的系统监控结束或删除作业进行之前询问密码，没有事前确认密码的户无法终止系统监控或执行某些特殊操作。

2.4.5 对病毒的确认及安全的修复选项

AhnLab Policy Center 2.0 扫描并确认文件有病毒感染，则立即进行自动修复以及其他相应措施。为防止可能发生的文件损伤,在修复之前,按用户设置将被感染文件另存到备份文件夹。针对不可修复的文件 AhnLab Policy Center 2.0 将这个文件删除以防病毒的扩散，删除前也可以保存到备份文件夹。此外，关闭 Windows 之前可确认是否受到病毒感染，由此可彻底阻断病毒的流入。

2.4.6 高效率防疫・管理的各种附加功能

利用高可信度的病毒分析技术及研究成果，安博士有限公司网页中病毒相关信息和病毒日历可帮助用户应付特殊的病毒。此外，为方便用户对产品的操作，AhnLab Policy Center 2.0 还提供扫描日志信息，各种环境设置选项，各种有用的工具菜单，有效地进行病毒的管理和查杀。

2.4.7 环境设置向导

AhnLab Policy Center 2.0 为不熟悉产品的用户，提供利用向导设置环境的功能，帮助用户设置环境选项，从而达到最优化的配置结果。

2.4.8 以迅速的升级维护系统安全

AhnLab Policy Center 2.0 与同类产品相比具有较快的升级周期(每周一次)，此外为解除用户每周手动升级的不便，智能升级应用程序中内置自动升级和预定升级功能。执行

智能升级应用程序可直接联接到安博士有限公司的互联网升级服务主机以及其它合作伙伴的服务主机并自动下载升级文件。

2.4.9 内置强有力的 WARP 引擎

利用安博士有限公司开发的 WARP 引擎，不仅对 Windows 平台，而且对 DOS 的内存区域也可进行彻底的病毒查杀，此外，它还提供国内外杀毒软件中最快的检查速度，完美的解毒率和文件恢复功能。

WARP 引擎是病毒查杀技术与预防技术相结合的杀毒引擎，它是整个网络防病毒系统的核心部分。它有以下的优点。

2.4.9.1 实时查杀各种病毒的防病毒功能

对于目前已被发现的国内外各种病毒，包括最近流行的恶性病毒（Back Orifice、CodeRed、Nimda、求职信等），它都提供 100%的检测，查杀功能。

2.4.9.2 出色的文件修复能力

具有出色的文件修复能力。为此可以使原文件受损程度减少到最小。

2.4.9.3 最快的查/杀速度

采用独特的修复方法（特定位置检查技术：只对具有被感染可能性的区域进行检查的方法），使它在目前市场上所有的杀毒产品中具有最快的查/杀速度。

2.4.9.4 对未知病毒的检测功能

不仅对已告知的病毒，而且对于未发现的病毒，也提供检测和处理功能。

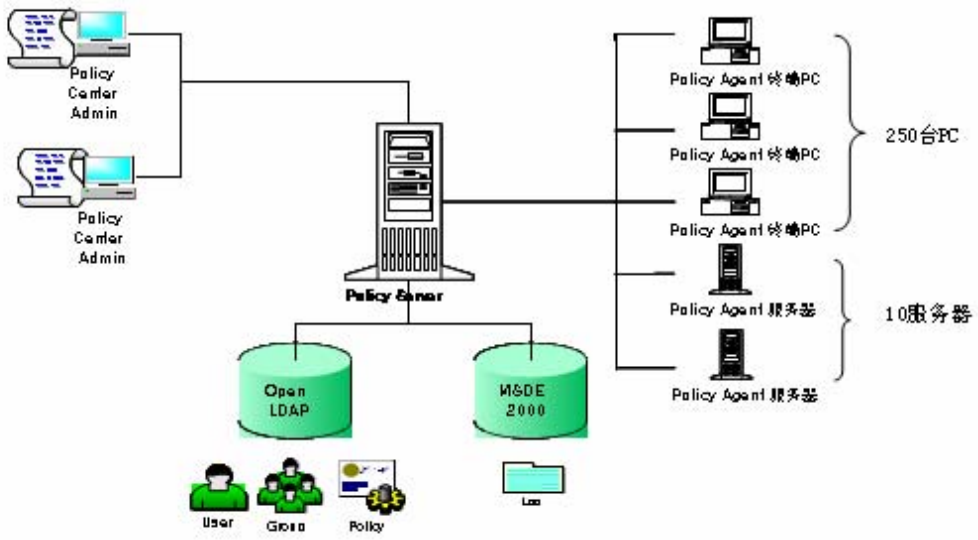
3 V3 系列网络防病毒系统的网络结构及组成

AhnLab Policy Center 2.0 软件是针对多种多样的企业环境对各种安全产品进行管理的需求而设计的统一管理方案。根据该设计，可以将多个安全产品所提供的共同的要素统一到一个平台之中，并使它们包含在一个统一的结构中，但是同时却使各产品所具备的固有的安全域能够有效地运行。

3.1 AhnLab Policy Center 2.0 的结构

AhnLabPolicyCenter2.0 软件从大的方面可以由三个层次结构来表示，即安装于管

理对象服务器的 PolicyAgent,安装于管理服务器的 PolicyServer 及数据库服务器，以及安装于管理员计算机的 Policy Center Admin 等三个层次结构(3-tier)。尤其是中央服务器除了 Policy Server 以外，还包括提供网络服务和 FTP 服务并行使 IIS 服务器和数据存贮器功能的 OpenLDAP 和 MSDE。



PolicyServer 将从管理员控制台 PolicyCenterAdmin 那里接受指令并需要进行处理的用户、组群、策略信息存贮于 LDAP 的记录中。并将这些信息通过 Policy Server 服务根据不同的用户或组群传递给相关的 Policy Agent。 Policy Agent 将把生成 的各种信息再传送给 Policy Server 并存贮于数据库中 。 Policy Center Admin 把存贮于数据库的内容，通过各种管理界面及报告，显示给管理员。

3.1.1 管理对象系统构成要素

- Policy Agent

Policy Agent 是安装于成为管理对象的计算机中，与中央 Policy Server 保持联系的程序。它将从 Policy Server 接收来的策略应用于各个安全产品。并且将从安全产品中获取的已经发生的各种登录及环境信息传送给 Policy Server。Policy Agent 由作为作业程序

的主要代理服务程序，和控制各种安全产品的各个代理模块组成。

- **个人安全产品**

个人安全产品是以独立的形态存在的 AhnLab 的安全产品，可以在 Windows 操作系统中单独进行运行操作。Policy Agent 所控制的安博士有限公司的安全产品有反病毒程序 V3 Virusblock, V3 Virusblock for Windows Server。

3.1.2 管理员系统的构成要素

Policy Center Admin 在管理员系统中全面执行运行作业的程序是 Policy Center Admin。它将 中所生成的安全产品运行策略及命令传送给服务器，并对从服务器接收来的各种信息进行处理，然后向管理员提供信息。

3.1.3 管理服务器系统构成要素

- **Policy Server**

安装于中央服务器的程序 Policy Server 集合了 NT 服务程序，而后者将 AhnLab Policy Center 2.0 软件的各种构成要素有机地联结起来。

Policy Server 大体上由下列五种形式的服务组成：第一是与各 Policy Agent 保持联系并对其请求做出回应的代理服务；第二是向 Policy Center Admin 传送主要 的数据并接受指令的控制台代理程序;第三是将从代理程序那里发送来的登录信息汇集起来并向上一域级传送的登录管理器；第四是为向代理程序发送服务器作业而进行调配的作业调度程序；第五是对服务器的程序进行生成、修改和删除的程序服务。

- **其他外部服务程序**

尽管 PolicyServer 本身不是组成程序，但是 PolicyServer 为了对大量的代理程序实施稳定的管理，而使用了已得到市场检验的三种服务器服务程序。首先，利用 FTP 协议传送文件，并使用了微软公司的 IIS 服务以通过网络服务提供所需要的信息。其次，对个别 Policy Agent 用户信息、组群信息、策略信息及服务器与代理程序通信环境信息等阅览为主的信息，使用了 LDAP 存储器。在 AhnLab Policy Center 2.0 软件中所应用的 LDAP 存储器，使用了开放资源方案的 OpenLDAP 服务器。在 OpenLDAP 中，拥有安全策略、用户信息、软件/硬件信息、组群信息、管理员信息、事件信息，以及其他环境设定信息等。

安全登录及事件信息等大量信息，使用了联结型数据库 MS-SQL 服务器。生成各种数据库表格并保存记录信息和状态信息，以操作提示的形式用于调度运行。

3.2 产品的结构特征

AhnLab Policy Center 2.0 软件作为将各种安全产品的策略统一于服务器实施管理而设计的产品，其在结构上具有如下一些特征：

- 基于目录服务的充分的策略服务器结构

AhnLab Policy Center 2.0 软件采用了扩展性和充分性超众的 LDAP 目录服务，利用 OpenLDAP 目录服务，使您可以方便地对复杂用户、组群信息和产品信息、策略信息 和 其相互关系等进行操作。通过具有扩展性设计的 Policy Server，可以使用户充分地对今后产品的升级及设置的修改等进行操作。

- 利用 RDBMS 的稳定的服务器运行

AhnLab Policy Center2.0 软件的 PolicyServer 为了实现大容量的数据处理，而使用了联结型数据库，可以对代理程序中生成的实时登录及事件等各种信息进行存储和加工。与 AhnLab Policy Center 2.0 软件联动的数据库，是 MS-SQL Server 7 及 MS-SQL Server 2000 。特别是为了降低中小规模用户采用 MS-SQL 的费用负担，在 AhnLab Policy Center 2.0 软件中提供了 MSDE 2000 程序。

- 充分的即插型结构管理域

AhnLabPolicyCenter2.0 软件的管理域根据安全产品的不同，而由三域和作为附加功能的磁盘管理功能等组成，拥有总共四个管理域。

各个管理域在安装 Policy Server 时进行选择。而且所选择的管理域在运行时，也可以根据组群或代理程序的不同，按照管理员的选择，随时地进行添加和删除。AhnLab Policy Center 2.0 软件虽然通过统一后的管理员界面提供各种安全产品，但是各个安全产品却可以根据用户环境的不同而方便地添加和充分运行。

- 智能型代理程序结构

PolicyAgent 安装于管理对象计算机中，并根据服务器策略的不同而对安全产品实施管理。按照 PolicyAgent 的自身高度作业，不断地对 PolicyServer 的变更事项进行更新，以使公司内部的安全策略与计算机内部的安全产品的策略，保持一致。PolicyAgent 可以对

相关系统所需要的各种安全产品的安装程序自动地进行下载和安装管理。

- 统一登录管理

将作为安全管理系统的重要功能的相关系统实时监控、统计、分析等一系列功能统一起来，在一个管理界面中加以显示。

- 具有扩展性的结构

即插型结构设计，可以对今后将要添加的安全产品便捷地提供帮助。AhnLab Policy Center2.0 软件是为了实现统一安全管理而考虑到扩展性的产品设计。这使得应对目前 还不存在的安全威胁的各种新型安全产品在面世时，也可以使用 AhnLab Policy Center 2.0 软件进行统一的管理。

- 具备充分性的不同产品安全管理

AhnLab Policy Center2.0 软件可以对多种安全管理要求充分地进行程度调节。AhnLab Policy Center2.0 软件都可以同时对这些要求加以满足。

AhnLab Policy Center 2.0 软件根据充分的代理程序设定策略，轻易实现了适合企业的安全方针的策略。

- 基于策略的安全管理平台

安全管理员通过存储事先定义好的安全策略，就可以将安全管理的大部分任务交由智能型的 AhnLab Policy Center 2.0 软件来操作管理。管理员所定义的多种安全策略和执行对象，存储于中央 LDAP 的存储器中，大部分的安全作业便可以实现自动地运行。管理员在需要对引擎进行更新时，或需要运行实时监视开启命令时，就不必要重复地进行机械管理操作。但是在对公司内部需要适用的组群和个别策略进行决定和定义时，因为其是主要任务，就可能需要在生产性业务上花费更多的时间。

- 应用于下级分散的层次性结构

AhnLab Policy Center 2.0 软件支持层次性服务器结构，以适用于拥有大量管理对象系统的大型企业。在拥有众多管理对象系统时，引擎文件的配置作业等可能会给系统及 WAN N/W 带来负担。因此通过将管理对象系统分散到复数 Policy Server 中，对 Policy 服务器间的层次结构加以定义，以同时满足下级分散和程序管理这一难题，实现对多个系统的管理。

4 V3 群件服务器防护系统介绍

随着群件系统在企事业单位的广泛使用，通过群件系统传播的病毒也日益增多。邮件、告示栏、共享文件夹等组件的基本功能在企业业务中的使用的同时，这也成为病毒的主要传播途径之一，因此多数企事业单位都开始部署对群件系统的病毒防护工作。

安博士更具用户的这种需求，开发出 V3NetGroup for Lotus Notes、V3NetGroup for MS Exchange 2003 两种使用最广泛的群件服务器系统的病毒防护产品。其优异的结合性，出色的稳定性得到用户的好评。

4.1 V3NetGroup for Lotus Notes 介绍

V3NetGroup for Lotus Notes 是利用 Notes/Domino 服务器在使用邮件及组件的企业环境中运行的防病毒软件产品。Lotus Notes/Domino 服务器是在全世界广泛使用的组件产品，它是为企业内的共享信息及共同工作使用的工具，并且把企业的指点资产集成在一起的部分，所以安装防病毒软件是非常重要的。

V3NetGroup for Lotus Notes 是在基准的产品中进行实时检查并确保产品的安全性，同时针对多种邮件病毒提高邮件过滤功能的升级软件产品。

4.1.1 主要功能介绍

- **正确而迅速的防病毒功能**
  a) 病毒实时检查, 预约检查, 手动检查
  b) 指定预约设置日期(每日, 每周, 每月, 指定日期)及设置检查运行时间的功能
  c) 支持多种压缩文件格式(27 种类)
  d) Incremental 检查功能(手动检查及预约检查时,只对检查日期以后的文件进行检查的功能)
  e) 邮件 Stamp 功能(在程序内部,安全的确认邮件的功能)
- **多种内容过滤功能**

a) 附件格式及邮件名过滤(选择及输入)

b) 邮件标题过滤 (不包括邮件本文的过滤)

c) 邮件尺寸过滤

d) 邮件发信人及发信域过滤

- **方便的管理功能**

a) 自动引擎升级

通过网络自动升级, 预约升级, 手动升级

局域网升级(目录升级)

b) 记录管理功能

事件记录(日期, 服务器类别)

病毒记录(日期, 服务器, 数据库, 检查方法类别)

邮件过滤记录(日期, 服务器, 收件人类别)

c) 备份管理功能

d) 被病毒感染时, 发送警告邮件

被病毒感染时,发送警告邮件(收发人, 管理员)

根据过滤阻断时, 发送警告邮件(收发人, 管理员)

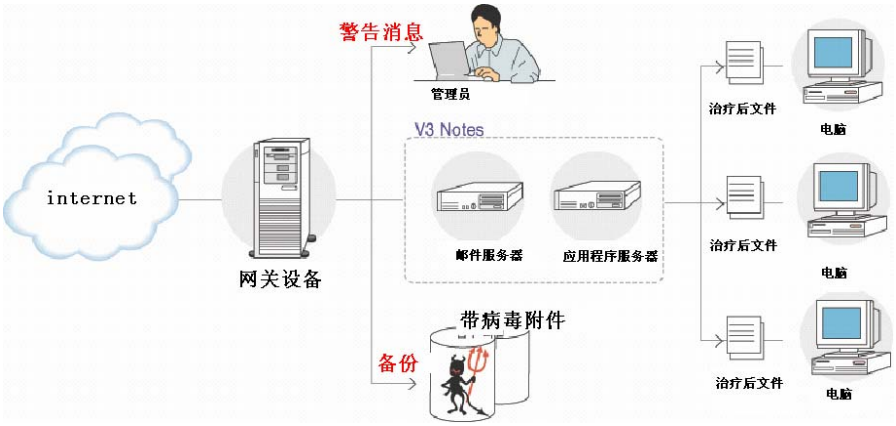
警告邮件编辑功能(标题, 正文)

e) 提供病毒日记及病毒信息(主页连接)

f) 实时监视服务器状态的功能(正在使用的引擎信息和产品版本,病毒检查状况等)

4.1.2 产品特点

V3Notes 是安博士有限公司开发的 V3 系列产品之一是基于 Microsoft Windows NT 4.0, Windows 2000 Server(MS Windows 2000 Server) 操作系统 Domino/Notes 服务器中操作的防病毒产品。Lotus 公司的 Domino/Notes 是全世界都认可的群件产品，帮助企业更有效地处理信息，共享信息。但是，由于没有防病毒功能，因此需要 V3Notes 的帮助。V3Notes 是基于 Domino/Notes 的企业网中彻底拦截病毒，发现病毒时提供最完善的诊断治疗功能。实时拦截被感染的邮件，并向管理员通知。



[图 4-1] V3Notes 系统组成图

- **完全保护群件服务器**

V3Notes 安装在 Domino/Notes Server，24 小时进行监视，因此不仅拦截流入 Domino/Notes 服务器的病毒，而且还阻断安装 V3Notes 之前已感染病毒向客户端的扩散。若与单机版防病毒产品 V3VirusBlock 一起使用，则从服务器的网络驱动器到客户端本地驱动器都能彻底拦截病毒。

- **嵌入安博士有限公司专有的先进 Wrap 引擎**

V3Notes 采用安博士公司开发的先进 Wrap 引擎® (WARP Engine : World-class Accelerated Recovery Processor)，国内外防病毒软件中最快，最准确的治疗（恢复）。Wrap 引擎是结合诊断/治疗和预防病毒技术的防病毒软件的核心部分，主要具有如下特点。

a) 立即响应病毒

不仅 100%诊断/治疗目前为止发现的国产病毒，而且还能彻底阻断国内外传播的病毒，最近从海外流入的宏病毒，蠕虫，后孔，后门等各种恶性病毒。安博士有限公司每周至少一次以上提供 V3Notes 升级，加强防护能力！

b) 出色的文件恢复功能

治疗被病毒感染文件时，具有出色的文件恢复功能。因此可最小化原文件的破坏损失。

c) 最快的诊断治疗速度

采用安博士公司专有的防病毒算法(检查指定位置技术:只挑选检查有可能被感染领

域的追踪算法)，比其它防病毒软件更快地诊断治疗病毒。

d) 诊断未发现病毒

不仅检查已知病毒，还能检查 1 万余种未发现病毒，更彻底地拦截新病毒的流入。

- **通过迅速升级，完全阻断病毒**

包括V3Notes的安博士有限公司的V3系列产品在国内外防病毒软件中具有最快的升级周期（每周一次）为解除用户每周手动升级的不便，在智能升级魔法师中嵌入了自动升级及预约升级功能。运行智能升级魔法师，则通过安博士有限公司的升级服务器及其它多个网络公司的服务器具自动下载运行引擎升级文件。

- **通过智能化实时检查，24 小时后台操作**

V3Notes 在 Domino/Notes 服务器中运行时，若试图从 Notes 客户端访问服务器，V3Notes 为拦截病毒运行智能防护功能。即，利用 Notes 客户端访问 Domino/Notes 服务器邮件，公告栏时监视预防 Notes 数据库中保存的文件是否被感染。利用 Domino/Notes 服务器访问互联网邮件时也相同。V3Notes 通过自身监视服务器功能，后台 24 小时在服务器运行，实时检查从外部到服务器的文件访问或文件的复印、移动、复制，最小化服务器的负荷。除此之外，通过手动检查，预约检查等检查功能的环境设置，使用多种检查方式。

- **检查病毒时，提供正确、安全的治疗选项**

V3Notes 经过检查确认被病毒感染，不仅自动进行治疗，还提供相应治疗的安全措施。V3Notes 根据用户选择，进行治疗之前，以防文件受损在 Notes 数据库中保存原文件。并且对于不可治疗文件，同样自动删除之前保存到 Notes 数据库。

- **为构筑完善的防护体系，提供检查记录及病毒信息**

管理员(Administrator)管理 Domino/Notes 服务器的邮箱时，V3Notes 为感染文件构筑体系的响应策略及跟踪感染路径提供检查记录，病毒信息，附加环境设置选项。根据网络状态，通过必要的检查治疗选项和环境设置，更有效地管理和控制网络。

- **根据指定条件检查删除相关文件的邮件过滤功能**

V3Notes 根据管理员(Administrator)设置的标题过滤，删除指定单词（句子），发送人地址，指定文件名或文件格式的附加邮件的过滤功能。对于确认已感染的文件，事先进行删除，减少服务器的负荷，提高检查病毒的速度。

4.2 V3NetGroup for MS Exchange 介绍

V3NetGroup for MS Exchange 2003 适用于，通过 MS Exchange 服务器使用邮件以及组件的企业环境中可以使用的病毒防御产品。V3NetGroup for MS Exchange 2003 防御外部的病毒感染邮件，防止内部用户之间的邮件来扩散的病毒，最终提高企业生产性的产品。如果同时使用本产品和 V3Net for Windows 服务器，就可以更加完整的保护 MS Exchange 服务器的信息。

4.2.1 主要功能介绍

- **正确迅速的病毒防御功能**
  - a) 实时病毒检测
  - b) 手动检测、预约检测(每天、每周、每月、指定日)
  - c) 选择检测对象以及文件形式
  - d) 压缩文件、宏检测
  - e) 支持多种压缩文件形式(27 种)
  - f) 病毒诊断时邮件删除、附件治疗/删除/备份/备份后删除的组合
- **内容过滤功能**
  - a) 附件名过滤(选择以及输入)
  - b) 邮件题目过滤
  - c) 附件尺寸过滤
  - d) 发件人过滤
  - e) 发件域名过滤
  - f) 邮件正文过滤
- **方便管理员的管理功能**
  - a) 自动引擎更新
    - ◆ 通过互联网自动更新
    - ◆ 预约更新/手动更新/本地更新
  - b) 日志管理功能
    - ◆ 事件日志

- 检测日志(病毒日志、邮件过滤日志)

c) 警告信息/MSN 服务

- 感染病毒时发送邮件(发件人/收件人、管理员)
- 邮件过滤后切断时，发送警告邮件(发件人/收件人、管理员)
- 警告邮件编辑功能(题目、正文)

d) 警告通知功能

- 根据指定时间内发现的病毒/邮件过滤数量，通过邮件和 MSN 服务通知管理员。

e) 设定复制功能

- 环境设置值，适用到其他服务器的设定复制功能。

f) 使用引擎信息(使用中的引擎信息和产品版本)

4.2.2 特点介绍

V3NetGroup for MS Exchange 2003 是安博士有限公司开发的 MS Exchange 邮件服务器防护产品，是在 MS Exchange Server 2000 及 2003 中运行的防病毒产品。MS Exchange Server 是全球广泛使用的 messaging 产品， 共享企业内部信息，更有效、更迅速处理业务。但是，随着通过 MS Exchange 共享企业信息及业务的增加，被病毒感染的危险性越大。要保护使用 MS Exchange Server 的 Messaging 系统的信息，则 V3NetGroup for MS Exchange 2003 中提供的病毒的诊断及汉治疗是必不可少的。

- **Messaging Sever 中拦截病毒**

V3NetGroup for MS Exchange 2003 针对安装在 MS Exchange Server，通过 ExchangeServer 接收，发送的信息进行诊断/治疗，从而完全拦截通过 Messaging Server 的病毒的流入及扩散。

- **使用安博士有限公司固有的优秀引擎**

V3NetGroupforMSExchange2003 使用安博士有限公司固有的优秀引擎，确保迅速、正确的治疗及恢复。利用安博士有限公司固有独资技术开发的该引擎是结合病毒诊断与治疗，预防技术的防病毒软件，大体具有如下优点：

a) 即时响应病毒的防病毒功能

不仅对到目前为止发现的国内病毒提供优越的诊断、治疗功能，而且对国内外流行的病毒，从海外流入的最新恶性病毒也诊断、治疗。

b) 治疗感染文件时的突出的文件恢复

治疗被病毒感染的文件时，具有突出的文件恢复功能。因此最小化对原文件的损伤。

c) 最快的诊断、治疗速度

利用安博士有限公司固有的防病毒算法(指定位置检查 ： 只选择有可能被病毒感染的领域进行检查的跟踪算法)，提高诊断、治疗的速度。

d) 诊断未发现病毒

对于国内/外目前未发现的病毒也提供诊断功能，彻底防护新病毒的流入。

e) 以迅速的智能升级魔法师，让新种病毒无效

包括 V3NetGroup for MS Exchange 2003 的安博士 V3 产品提供定期升级(每周 1 次)和非定期升级(随时)，为解除使用者手动升级的不便，产品还提供智能升级魔法师。智能升级魔法师® (Smart Update)是,安博士有限公司开发的固有的服务，通过互联网自动下载引擎升级文件，信息等，自动安装用户的服务器系统。

f) 准确、安全治疗检测病毒

V3NetGroup for MS Exchange 2003 确认被病毒感染，则不仅自动治疗病毒，还能提供安全对策。V3NetGroup for MS Exchange 2003 在治疗病毒之前，为了避免文件损失，复制原文件或对于不可治疗文件进行自动删除，防止病毒的扩散。

g) 构筑彻底防护体系的检查日志，病毒信息

V3NetGroup for MS Exchange 2003 提供病毒检查日志，病毒信息，多种检查选项，根据 MS Exchange 服务器的负荷和网络状态，更有效地管理及运营。

h) 为更稳定的实时检查，支持VSAPI

V3NetGroup for MS Exchange 2003 为更稳定地实时检查，支持微软提供的 VSAPI(Virus Scanning Application Program Interface) 2.0 及 2.5。VSAPI 2.0 是在 MS Exchange 2000 服务器 SP1 以上操作, VSAPI 2.5 是 MS Exchange 2003 以上操作。使用 VSAPI 模式，则对于进入/出信息存储所(IS ： Information Store)邮件和信息，诊断/治疗病毒。

5 V3 网关邮件防病毒系统介绍（SMTP 协议）

V3GateBlock Email(SMTP) for Windows Server 通过邮件(SMTP)服务器的安全策略应用，根据安全策略，防止有害邮件流入，流出网络。使用 V3GateBlock Email(SMTP) for Windows Server，实时检查流入或流出感染邮件的路径，拦截邮件感染扩散，保护网络与用户计算机环境。并且利用内容过滤功能与邮件拦戴功能，彻底拦载对安全造成威胁的邮件进入网络的路径。

5.1 V3GateBlock 产品功能和特点介绍

- **强大的防病毒功能**
  a) 利用 WARP 引擎迅速正确地检测病毒
  b) 检测被感染的文件之前，对原文件进行备份
  c) 被感染时，向管理员，收信人，发信人发送警告邮件
  d) 提供通过 VIP 的功能
  e) 在指定时间自动升级引擎的预约升级功能
  f) 附件文件包含宏功能时，删除宏功能，传送邮件的功能

- **保护多种邮件的功能**
  a) 对邮件主题及内容的目录过滤的
  b) 过滤受限邮件的大小
  c) 事先检测管理人员设置的附件文件名或扩展名的文件过滤功能
  d) 过滤垃圾邮件的功能
  e) 通过阻断目录事先能组断威胁安全的邮件
  f) 自动升级阻断目录

- **灵活的适用性**
  a) 设置路由器的功能支持所有邮件格式的解决方案
  b) 支持多重 SMTP 服务器
  c) 支持多种 UNIX, LINUX 服务器

- **顾虑使用者的方便，设置有效的对策**
  a) 按个人、域名、IP 的不同，制定不同的病毒防御策略
  b) 可针对病毒检测或治疗设定多种不同的检测策略
  c) 可根据轻重缓急设置优先任务，从而使多种多样的防毒之策能达到最佳效果
  d) 可按 IN-BOUND/OUT-BOUND 的不同适用于不同策略
  e) 对邮件大小，标题和本文，附件文件，垃圾邮件设置过滤策略

f) 提供通过 VIP 的功能

- **有效的管理功能**

a) 启动系统时可执行默认的防毒策略且没有任何漏洞
b) 提供基于网页的方便的管理工具
c) 提供多种检测或事件记录的管理功能和逐项统计功能
d) 检查病毒及按接送信者的不同统计功能
e) 警告邮件的功能
f) 实时监视功能

6 安博士在线安全产品介绍

6.1 网络在线安全现状

由于互联网络的发展，整个世界经济正在迅速地融为一体，而整个国家犹如一部巨大的网络机器。计算机网络在经济和生活的各个领域正在迅速普及，整个社会对网络的依赖程度越来越大。众多的企业、组织、政府部门与机构都在组建和发展自己的网络，并连接到 Internet 上，以充分共享、利用网络的信息和资源。网络已经成为社会和经济发展强大动力，其地位越来越重要。伴随着网络的发展，也产生了各种各样的问题，其中安全问题尤为突出。

网络面临的主要威胁主要来自下面几方面:

1) 黑客的攻击

黑客对于大家来说，不再是一个高深莫测的人物，黑客技术逐渐被越来越多的人掌握和发展，目前，世界上有 20 多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用以及系统的一些漏洞，因而系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性好，“杀伤力”强，是网络安全的主要威胁。

2) 网络的缺陷

因特网的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的 TCP/IP 协议族，缺乏相应的安全机制，而且因特网最初的设计考虑是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此它在安全可靠、服务质量、带宽和方便性

等方面存在着不适应性。

3) 软件的漏洞或“后门”

随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免的存在，比如我们常用的操作系统，无论是 Windows 还是 UNIX 几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件、等等都被发现过存在安全隐患。大家熟悉的尼母达,中国黑客等病毒都是利用微软系统的漏洞给企业造成巨大损失,可以说任何一个软件系统都可能会因为程序员的一个疏忽、设计中的一个缺陷等原因而存在漏洞，这也是网络安全的主要威胁之一。

4) 用户自身的失误

网络内部用户的误操作，资源滥用和恶意行为再完善的防火墙也无法抵御来自网络内部的攻击，也无法对网络内部的滥用做出反应。

6.2 MyV3 在线杀毒

6.2.1 MyV3 的基本概念：

无需安装杀毒软件，只需登陆互联网就能享受查杀病毒的服务，使您安全的使用您的电脑。

6.2.2 MyV3 的主要功能：

1) 互联网端口检查

彻底切断通过当前使用端口活动的 Backdoor 程序（Back Orifice 等），切断系统及用户信息泄漏。

2) 检查引导区域

检查当前使用中的系统引导区域病毒感染与否。

3) 内存区域检查

检查当前使用中的系统内存区域病毒感染与否。(可以根治 CIH 等感染内存区域的病毒，将病毒的再次感染率降低到最低。)

4) 压缩文件检查

检查扩展名为 ZIP, ARJ, RAR, JAR, CAB, LHA UUEN/DECODE, ZOO. MINE 的压缩文件。基本/扩展模式，根据需要可以选择设置状态(选择扩展模式时，除了基本检查、

检测/清除功能之外，可以指定检查设置、文件格式、清除设置等)

6.2.3 MyV3 的系统特征

1) 不需要另外安装，只要登陆互联网就能查杀病毒。(ActiveX 模块)
2) 可查杀本地驱动器及网络驱动器。
3) 内载 WARP Engine，提供迅速而准确的查杀功能。
4) 治疗感染文件时提供出色的文件修复功能。
5) 始终执行自动升级，确保使用最新版本的杀毒软件。
6) 简便的用户界面。

MyV3 的执行过程：

服务器端执行过程：
需 ASP 环境服务器（10M）
调试脚本程序
客户端 IE、NETSCAPE 浏览器登陆
客户端下载程序

客户端执行过程：
客户端 IE、NETSCAPE 浏览器登陆
认证服务器验证
检测最新升级文件
执行程序

6.2.4 MyV3 的优点

1) 简便的使用方法

登陆的同时升级引擎，因此只要有互联网环境及 Web 浏览器，不论何时何地都能使用最新版本的查杀引擎。而且 MyV3 是利用 ActiveX 技术自动执行于 Web 浏览器，因此不需要另外安装程序。最初执行 MyV3 时，根据用户环境，完成执行程序需要一定时间。

2) 友好的用户界面

MyV3 具有简单的用户接口及友好的设计，只要轻轻点击鼠标就可以完成从病毒检测到清除一系列的操作。而且可以通过 HTML 传达呼叫信息，因此仅仅通过链接等简单操作，也能够在主页上搭建 MyV3 服务环境。

3) 内置安博士有限公司独有技术力量研制而成的 V3 Engine

内载安博士有限公司的 WARP 引擎，可以稳定、快速地进行查杀，治疗感染文件时也

具有出色的修复功能。每当执行在线服务时都会使用最新版本的引擎，因此不需要作额外的引擎升级操作。具有快速的搜索功能，并且提供多种选项设置功能。

7 服务与支持

7.1 用户支持服务

计算机病毒的发展速度很快，因此反病毒产品的升级服务和技术服务就显得非常重要。鉴于此，安博士有限公司根据中国国情建立起一套完善的服务网络体系。除了提供传统的售前咨询、电话服务、电子服务等服务方式外，在主动服务方面，安博士有限公司开创了国内主动服务体系的先河，通过这项主动服务体系，用户无需自己上网升级，安博士有限公司的升级魔法师系统系统会通过互联网络自动将产品升级。

为了确保技术服务质量安博士有限公司还在全国各省的代理商中开通电话专线，专门用于处理用户意见的反馈。定期进行用户调查，以了解用户对安博士有限公司产品和技术服务的满意程度以及用户对服务的需求方向。通过总结，对安博士有限公司产品和服务进行调整，以满足用户各种不同的需求，真正做到将服务送到每一位用户手中，让每一位用户都满意。

7.2 技术支持与服务

技术服务联系方式：

1．提供电话技术咨询。

2．提供电子邮件咨询。

3．每周通过网络升级病毒库和产品。

8 附录

8.1 国内外主要客户名录

首都在线　　三星集团

上海热线	LG 集团
深圳热线	SK 集团
武汉热线	现代集团
重庆热线	韩国第一银行
上海市人民政府	韩国政府
中国公安部	Woori 银行
清华大学	韩国保险
上海交大	现代保险
浙江大学	Daum.net
中国移动	现代股份
中国电信	马来西亚警察总署
中国税务	BIGLOBE
中国网通	FUJITSU
中国电力	NTT
交通银行	TOSHIBA
工商银行	SHARP
浦东发展银行	NEC
民航管理局	日立银行
胜利油田	美国花旗银行