白 皮 书

使用趋势科技防毒墙－服务器版（ServerProtect 5.0®）在文件所在的位置保护文件

趋势科技·中国
新趋网络科技（上海）有限公司
上海市淮海中路222号力宝广场511室
电话：021-53966800
传真：021-53966407
http://www.trendmicro.com.cn

目录

概述 3

为文件服务器提供保护 4

趋势科技防毒墙－服务器版（ServerProtect 5.0） 5

产品架构 5

管理控制台 6

信息服务器 6

标准服务器 7

主要特性和优势 7

快速、可靠的扫描引擎，最大限度减少系统效能降低事件的发生 7

自动、智能化更新病毒代码与程序文件 7

利用任务管理器完成自动的、可定制的病毒防护任务 7

事件通知 8

日志报告 8

小结 9

系统要求 10

关于趋势科技 11

2000 年 9 月（2001 年 7 月更新）

趋势科技・中国

新趋网络科技（上海）有限公司

在文件所在的位置进行保护

概述

随着病毒的日益猖獗，防毒软件必须能够创建和维护一个无病毒的网络环境，这一点非常重要。由于一个企业大部分的宝贵资产都包含在它的相关信息中，因此，需要保证数据的完整性和数据本身免遭病毒的破坏。对于文件服务器来说，安全性和数据的完整性非常重要。趋势科技防毒墙－服务器版（ServerProtect 5.0）可以保护整个网络的文件服务器，它采用了最先进的病毒防护技术以确保你的网络不受病毒的侵扰。

本文件对为服务器提供防毒解决方案的重要性进行了阐述，并对趋势科技防毒墙－服务器版（ServerProtect 5.0）的三层式软件架构如何保护服务器的问题进行了探讨。

为文件服务器提供保护

病毒对网络的攻击正变得日益普遍、频繁和猖獗。内部网络和网络连接（尤其是与互联网和内部网相关的网络连接）的快速增长使病毒事件发生的数量也不断增长。不仅病毒侵入企业的方式在不断增多，病毒事件发生的频率也在增加，这主要是因为新型病毒的不断出现，如宏病毒和 PE 类型的病毒，它们可以通过共享文件或电子邮件/附件快速传播。

用户共享的文件越多，被病毒感染的机率就越大。然而，感染机率的不断增长并不是联网环境中管理人员所面临的唯一问题。病毒感染造成的影响及其广度不但直接给企业造成破坏，而且增加了企业因清除病毒而造成的额外成本支出。

在一个非联网的环境中，病毒通常是经由软盘来传播的，并且只限于那些使用软盘的计算机。假使病毒没有被发现，那么要感染办公室内的所有计算机，通常需要几个月的时间。然而，在联网环境中，由于网络能够快速、高效地共享文件，因此，那些进入网络的病毒便能够在几个小时内感染办公室内的所有计算机。所以，在一个联网的环境中，因为病毒传播的速度极快，很难有机会对被感染机器进行隔离。而这一切都是由网络服务器所引起的。

一个受病毒感染的文件可以使文件服务器中的大量数据被传染，这会导致企业网络文件存取和文件管理系统的灾难性崩溃。被感染的文件可能会被许多网络用户所检索，最后通过电子邮件或直接下载传播到其它的客户系统或公司。

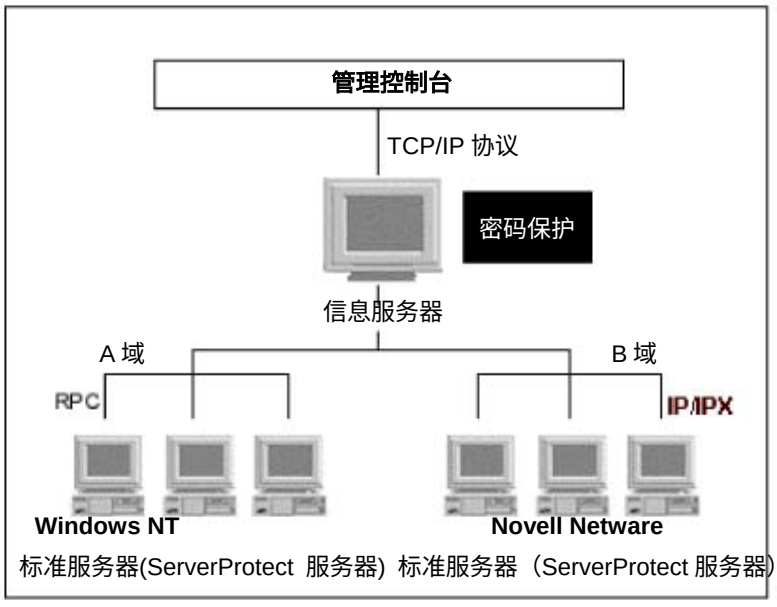
趋势科技防毒墙－服务器版（ServerProtect 5.0）

趋势科技意识到，互联网环境需要一个强大、可靠的病毒防护解决方案，并且需要用到趋势科技协助 Intel®和 Novell®等公司开发防病毒软件所获得的宝贵知识和经验，借助这些开发经验，趋势科技为 NT 和 Netware 服务器构建了新一代的病毒防护方案。趋势科技防毒墙－服务器版（ServerProtect）是一个基于服务器的病毒防护方案，可以检测到已知和未知的病毒，甚至是未知的宏病毒。ServerProtect 可以用最低的执行和管理成本提供最全面的病毒防护。

考虑到内部网络不断增长和日益复杂的因素，ServerProtect 还提供防毒软件管理功能，以降低管理成本。对于那些位于企业局网（LAN）、广域网（WAN）和内部网（Intranet）的基于 Windows NT 和 NW 的服务器，ServerProtect 满足了他们的防毒需要。趋势科技可靠的病毒扫描技术以及集中的域管理和软件分配功能为你提供了一个强大的防毒工具，保护你的电子资产免受病毒的破坏。

产品架构

ServerProtect 是通过一个 3 层的结构为网络提供病毒防护的：管理控制台、信息服务器、标准服务器。管理员可以利用管理控制台配置信息服务器（IS），然后利用信息服务器控制 IS 域内的标准服务器。



1． ServerProtect 通过一个三层式的架构来实现整个网络的安全管理：管理控制台、信息服务器和标准服务器。

ServerProtect 允许远程管理的远程和便携式控制台大大方便了管理员的管理活动。

新的架构提升了远程和域管理功能

特性

- 通过远程控制台对 Windows NT 和 Novell Netware 服务器进行集中管理，管理员可以通过一个 32 位 Windows 主机上的便携管理控制台管理多个服务器。
- 管理控制台和服务器中防毒程序之间的实时双向通讯使 ServerProtect 能够监测连接情况，处理扫描请求，返回扫描结果。

优势

- 用单一控制台管理 NT 和 NW 服务器，减少了在不同服务器之间反复切换所花费的时间和精力。利用集中控制功能，管理员可以轻松完成以下任务，如，配置扫描、病毒类型和程序文件更新、编辑病毒记录、设置实时扫描参数。
- 可以对 ServerProtect 进行远程安装、维护、升级和卸载，使管理员能够同时管理多个服务器。
- 利用 ServerProtect 的集中管理功能，管理员可以进行实时扫描、更新，可以为所有服务器配置修改信息，以确保在病毒爆发时，所有服务器都采用的是最新的病毒防护程序。
- 可立即对病毒活动提供反馈，有利于发现潜在的安全漏洞，使管理员轻松管理存储数据的完整性，防止恶意代码进入网络的其它部分。
- 最大限度地减少了控制台与服务器之间所需的通讯延迟时间，减少了病毒传播危险，确保了稳定的病毒防护。

此外，信息服务器的安装方便了对域的管理，一个域内的所有服务器都能共享相同的配置和相同的更新。共享相同的更新还将节省互联网的带宽。ServerProtect 是市场中唯一一个使用单一控制台同时管理 NT 和 Netware 服务器的产品。

管理控制台

ServerProtect 管理控制台是一个便携式的控制台，它能够使网络管理员集中控制多个网络服务器和域。管理员可以同时配置同一个域内的多个服务器，并可从所有服务器生成综合的病毒事件报告。

控制台由 4 部分组成：

- Outlook 快捷工具条
- ServerProtect 树状结构域
- 配置数据区
- 下拉式菜单

ServerProtect 的树状结构域用于显示所有的 ServerProtect 服务器，包括 NT 和 Netware 服务器，服务器的状态显示在标题栏上。状态内容包括病毒代码、扫描引擎和程序文件的版本，在网络中所发现的病毒的名称，操作系统的类型和版本，实时扫描的指示，清除病毒所采取的行动，等等。注意，上面的所有的状态信息都可以由 ServerProtect 用户自己配置。

信息服务器

信息服务器为它所管理的标准服务器处理关键性的信息和通讯。用户可以为信息服务器中的所有服务器配置信息，在信息服务器中，这些配置数据可以被共享和存储。

在文件所在的位置进行保护
标准服务器

标准服务器指得是安装了 ServerProtect 的 Windows NT / 2000 或 Novell Netware 服务器。在 ServerProtect 结构中，标准服务器的级别要比信息服务器低，并且是由信息服务器管理的。

主要特性和优势

快速、可靠的扫描引擎，最大限度减少系统效能降低事件的发生

ServerProtect 获得了 ICSA 认证，可以 100%地检测和清除所有已知病毒。ServerProtect 高效的扫毒功能可以为大多数压缩文件格式提供循环扫描，包括 ARJ, Diet, LZEXE, LZH, PKLITE, PKZIP 和 Microsoft Compress 以及 UUENCODE 和 MIME 邮件附件等。

由于 ServerProtect 能够与大多数常用的服务器应用软件兼容，所以保证了 ServerProtect 安全部署及业务应用的平稳运行。此外，ServerProtect 已经获得 Microsoft 的 Windows 2000 认证，保证了程序间的互操作性。

ServerProtect 采用了多线程的设计，可以有效的运用多处理器的计算功能，支持快速扫描，同时最大限度地减小了网络吞吐量和客户接入时间等性能降级事件发生的可能。

自动、智能化更新病毒代码与程序文件

自动更新保证了 ServerProtect 能够自动下载最新的病毒代码和扫描引擎文件，而不用管理员或用户的参与。向服务器交错发送更新通知使更新进程流线化，从而不会影响到网络的带宽。增量病毒代码更新为更新大量的服务器防毒程序提供了一个快速、高效的方式，尤其是对那些具有较慢连接速度的远程办公地点尤为有效。

利用任务管理器可完成自动的、可定制的病毒防护任务

ServerProtect 5.0 实现了一个任务导向的用户界面，使用户能够为一系列的执行动作创建一个批处理任务。这些任务可以在任何时间执行。一个 Windows 式的向导文件将指引用户完成任务创建过程。

对于任何一个任务，都有一个状态栏，用来提示这个任务是否正在执行或将要执行。在每个任务的前方都有一个对应的图标。

- 任务管理器可以对防毒维护进行标准化，节省配置的时间和精力。使管理员能够集中处理其它事务。
- 创建预配置的标准化任务，进行日常的防病毒维护活动和策略设定；新安装的服务器可以轻松继承原来的设定，以保证服务器间的一致性。
- 可定制的日常扫描任务能够使管理员为不同的群体创建不同的任务，以满足不同域的需要。

事件通知

ServerProtect 包含一个增强的通知模块，它在发生下列事件时将发出警报：病毒感染，运行或卸载 NT 服务／Netware NLM，配置变化、尝试修改被设定成“ 拒绝修改 ”的目录和过期的病毒代码等。警报可通过邮箱、寻呼机、打印机、互联网邮件、SNMP trap 或 Windows NT 事件日志发送。

用户可以选择在何种情况下发送警报。比如说，一个用户可以设置 ServerProtect，使他能够在发现几个病毒后或在一定的时间内接收警报信息。

日志报告

ServerProtect 的全面日志报告可跟踪和管理大量的病毒防护事件，包括病毒感染、类型或程序文件更新、病毒警告、运行任务、递交可疑文件、扫描活动和写保护文件夹被修改等。

ServerProtect 在记录报告中还提供以下内容：

- **感染**：病毒感染的状态
- **扫描总结**：实时扫描启动/停止，手动扫描启动/停止，定时扫描启动/停止
- **系统**：打开文件失败；系统消息
- **更新**：更新病毒代码/扫描引擎/程序补丁的结果
- **警报**：标准化的警报
- **任务**：任务执行的结果
- **采取的行动**：对一个被感染的文件执行的多个动作
- **感染源**：病毒进入网络的可能入口

ServerProtect 使用户能够对被感染的文件采取进一步的行动。包含将一个已清除文件恢复到原来的位置，删除一个清除备份文件，或将被感染文件的一个“ 清洁的 ”拷贝用电子邮件附件的形式发送给用户。

小结

随着电子邮件病毒的日益猖獗，防毒解决方案必须能够创建和维护一个无病毒的网络环境。对于文件服务器来说，安全性和数据的完整性非常重要，因此，应保证数据的完整性和数据本身不受病毒的破坏。

趋势科技防毒墙－服务器版（ServerProtect 5.0）采用了最先进的病毒检测技术，保证企业最宝贵的资产不会受到病毒的破坏。此外，ServerProtect 还能够让网络管理员从一个便携的管理控制台上对多个 Windows NT 和 Novell Netware(NW)服务器和域进行管理。这个控制台能够让管理员同时配置一个域中的多个服务器，并能够从所有服务器中生成综合的病毒事件报告。

系统要求

管理控制台

- Microsoft Windows 2000 Professional / Server (SP1, SP2), Windows 95/98/Me, Windows NT 4.0 (SP3或以上)。
- 支持800 x 600 或更高分辨率的显示器。
- 网络协议和服务：TCP/IP, Microsoft Network和RPC服务必须运行在安装后的服务器上。

信息服务器

- Microsoft Windows 2000 Professional / Server (SP1, SP2), Client 32。
- Microsoft Windows NT 4.0 (SP3或以上)。
- 64兆内存或更高。
- 50兆可用磁盘空间。
- Intel Pentium 166 MHz 或更快的处理器 (或同级产品)； 网络协议和服务：
  TCP/IP, Microsoft Network,适用于 Netware 和 RPC 服务的网关服务以及RPC服务。上述程序必须运行于上述平台安装后的机器上。

  对于Netware用户，须安装Windows NT或Windows 2000的机器作为信息服务器管理Netware服务器。

标准服务器

- Microsoft Windows 2000 Professional / Server (SP1, SP2), Microsoft Windows NT 4.0 (SP3或以上)。
- Novell Netware 3.12/4.x/5.x。
- 64兆内存或更高。
- 50兆可用磁盘空间。
- Intel Pentium 166MHz 或更快的处理器 (或同级产品)。
- 网络协议和服务：
  - TCP/IP, Microsoft Network, 和 RPC 服务必须运行在已安装的 Windows NT WorkStation/Server上。
  - IP 或 IPX/SPX 必须运行在已安装上述平台后的 Netware 服务器上。

关于趋势科技

关于趋势科技：
趋势科技于1988年在美国加州成立，分别在美国Nasdaq和日本东京证券交易所上市，是目前全球市值最高的防毒软件公司。趋势科技23个分公司遍布全球，包括中国，北美，欧洲，非洲，亚洲和澳洲。据IDC最新调查报告，趋势科技的网关级防毒软件、邮件服务器防毒软件和群组服务器防毒软件在全球市场占有率第一。