TREND MICRO

Product Paper

Office Scan 企业版 v3.0
技术白皮书

Trend Micro, Inc.

Trend Micro Incorporated, 10101 N. De Anza Blvd., Suite 400, Cupertino, CA 95014

Tel: (408)257-1500/1-800-2285651 Fax: (408)257-2003 www.antivirus.com

主从式架构的病毒防护

简介

计算机病毒不仅对计算机使用者造成危害，对于所有运用信息科技的企业亦构成威胁。这些透过磁盘共享档案、电子邮件讯息、线上通讯等方式进入计算机的恶意的程序， 可能在计算机中恣意破坏 – 有时会删除档案，重新格式化硬式磁盘驱动器，或是令硬件无法运作。新型态的病毒夹带着新科技出现 – 部分网站内嵌了恶意的 script 与控制组件，消耗计算机的资源，窃取密码或是您输入计算机中的其它机密信息.

Internet 及企业内部网络的迅速成长，传输进出企业工作站的档案数量随之大量增加。如此毫无限制的档案传输无异是提供了一个简便的机制供计算机病毒企业网络环境中散播，甚至往外扩散。

听完了坏消息，接下来是好消息：防毒软件业者已经发展出保护计算机或网络环境免于病毒侵害的产品，但是，***必须持续一致地使用***。然而许多计算机使用者与 MIS 人员皆认为防毒软件不是操作不易，就是对工作造成不少干扰。在美国，虽然中大型企业与政府机关中四分之三的计算机已安装防毒软件 ，感染病毒的比率仍持续升高；1997 年，在这些企业组织中，大约百分之四十的计算机受到计算机病毒感染[1]。目前的挑战是必须要发展出 不干扰企业员工工作的软件，将网络环境防毒策略交由公司的 MIS 专业人员集中控管。

病毒防护的传统处理方式

许多企业组织试图在公司内所有工作站中安装单机版本的防毒程序以对抗病毒的侵害。这些程序可保护单一的计算机，但无法提供任何集中的控管与报告。这种「膏药式」的解决方案对独立的单机或许有效，但却无法运用在企业网络环境中。

在网络环境中使用单机防毒程序，每一工作站的使用者依个人的喜好自行设定管理软件，设定并无一致性。部分使用者可能会移除或是关闭在他们计算机上执行的防毒软件，使他们的工作站无法受到保护。除此之外，运用病毒 signature 比对技术的防毒软件必须依赖最新的病毒码档案始能有效的发挥功用。姑且不论一个企业的工作团队了解安全防护的程度有多少，但是要每一个员工每个月二次从工作职务中抽出时间来下载新的病毒码档案，似乎是件不可能的事。

企业组织依赖员工的配合来管理公司的防毒策略是不切实际的。病毒威胁对公司造成的损失可能非常严重，管理阶层须重视这个问题，并由 MIS 人员须提供专属的资源。

集中控管的重要性

要防护网络环境免于计算机病毒的威胁必须详细了解病毒感染的特性。您必须知道病毒种类、感染数量、病毒藉以进入网络环境的漏洞。

要求每一个员工自行管理单机版防毒软件，无法取得网络环境病毒事件的整体报告。MIS 管理人员无从了解问题的 “概况”，因而严重阻碍了解决方案的产生。

主从式架构

Office Scan 企业版 专为保护工作站而设计，虽然不对档案服务器、电子邮件/群组应用软件或是 Internet 网关器提供防护，但可与趋势科技的其它产品结合以提供上述等区域的防护。此软件包含了二个主要的组件 –安装于公司内所有工作站的客户端程序，以及供系统管理者集中监视控管客户端程序的管理主控台。

单机版防毒软件将病毒扫瞄决策交付给工作站使用者，因为无法确定这些防毒软件的操作是否正确，并无法有效地保护网络环境。部分员工可能会移除或关闭防毒软件，或者忽略重复出现

的病毒感染警示。确保全面性网络环境安全的唯一方式是在公司内所有计算机中安装病毒扫瞄软件，并指定一位专责的管理人员监控此软件。

支持 Web-based 及 File-based 通讯协议

今日的企业网络环境通常混合了 Novell NetWare 与 Windows NT 网域。主从式架构防毒软件必须同时支持此二种网络通讯协议，而不受限于任何一种。

Office Scan 企业版 的管理主控台与客户端程序之间支持二种通讯协议。执行 Windows NT 4.0 加上 Microsoft Internet Information Server (IIS) v. 3.0 或以上版本的网络环境支持实时 HTTP 通讯以传递病毒事件记录资料，以及程序与病毒码更新。执行 file-based 通讯协议 (Novell NetWare) 的网络环境亦有支持，藉由服务器登录程序(server login script)传递信息。除此之外，file-based 网络环境中的客户端程序每小时会对设定信息数据库作一次轮询(poll)，查询设定是否有变更，或是否有新的程序更新档案或病毒码档案。

实时 HTTP 通讯提供防毒软件相当大的利益。系统管理者对网络环境的防毒活动可确实掌握状况，不受限于 file-based 通讯既有的时间延迟。此外，设定的变更与新的程序更新档案或病毒码档案可透过网络实时传递。Office Scan 企业版 运用了最新的科技，但也同时保留了与传统的 file-based 通讯协议的兼容性。

自动化传送病毒码档案与程序更新档案

当您安装了运用病毒 signature 比对技术的防毒软件，使用最新的病毒码档案是非常重要的。而依赖每一个工作站的使用者下载且更新病毒码档案是非常冒险的，因为您仰仗员工的配合，而这些员工可能工作繁忙且不十分重视网络环境安全。

趋势科技 Office Scan 企业版 可经由趋势科技网站、BBS 或是服务磁盘下载新的病毒码档案及程序更新档案，下载完成后，您可以通知工作站使用者。执行 HTTP 通讯协议的 Office Scan 网络会以循序的方式传送病毒码档案与程序更新档案，将网络传输负载降至最低。利用 file-based 通讯协议安装的 Office Scan 客户端程序会在下一次登入网络时或是每小时对服务器作轮询时收到更新的病毒码档案。

多重管道部署客户端程序

如果系统管理人员想要管理网络环境中每一台工作站的病毒防护工作，尽量简化客户端程序的安装过程是需要优先考量的。程序部署方式必须虑及工作站执行的不同操作系统平台。

Office Scan 企业版 提供了四种部署客户端程序至工作站的方式：编辑服务器登录程序(Login Script)、Web-based 部署、Windows NT 远程安装、及利用 Microsoft System Management Server (SMS)。服务器登录程序 (Login Script) 是网络环境中远程安装软件的传统方式，这种方式同时适用于 Novell NetWare 与 Windows NT 平台，而其它三种方式则仅适用于 Windows NT。

为了引导您完成客户端程序部署的程序，我们提供了一个完整的工具称为 Planning Manager，协助您完成客户端程序的预先设定与部署。

Planning Manager

Planning Manager 引导您进行下列工作：选择安装 Office Scan 客户端程序的工作站、将工作站加入本地端网域以简化管理工作、选择部署程序的方式、及部署客户端程序之前的预先设定工作。

Planning Manager 可确保客户端程序在一开始安装至目标工作站时，即确实设定为所需的方式。

编辑服务器登录程序 (Login Script)

利用工作站连接至服务器所执行的服务器登录程序 (Login Script) 进行远程安装软件，已曾被采用过，且是较实际的方式，同时适用于 Novell NetWare 与 Windows NT 平台。我们提供了一项工具协助您选择服务器然后编辑该服务器的登录程序 (Login Script)。

Web-based 部署客户端程序 (与 Web Deployment Sender)

符合实时 HTTP 通讯协议系统需求的 Office Scan 网络，在程序安装过程中，会显示安装客户端程序设定网页，此网页包含了一个 ActiveX 控制组件，会自动侦测每一台连接至此网页工作站的操作系统，下传并安装适用的客户端程序.

为了要通知工作站使用者有关 web-based 部署页面的信息，有一项工具称为 Web Deployment Sender 可协助系统管理者编写、搜寻地址及传送通知讯息至网络环境中的工作站使用者，告知有关此网页的讯息。Web Deployment Sender 适用于与所有 MAPI 兼容的电子邮件服务器软件。

Windows NT 远程安装

Windows NT 网络环境中的客户端程序可透过 Windows NT 远程安装来进行部署。这个工具可让您检视网络中所有的 Windows NT 网域、选择要安装及执行客户端程序的工作站。

Microsoft System Management Server 中的 Task

Office Scan 企业版 与 Microsoft BackOffice SMS 的标准兼容，因此您可以在 Windows NT SMS Asministrator 中设定一项 task，进行 Office Scan 客户端程序的部署。

Office Scan 管理主控台

双重管理主控台

为实现趋势科技针对企业防毒软件提供完整解决方案的承诺，Office Scan 企业版 提供了二种版本的管理主控台。一个是 web-based 的管理主控台，运用了 HTTP、HTML、Java 与 CGI 等标准的网络科技所创造出来含有多种功能的管理主控台，可利用网络浏览器来存取。另一个管理主控台为标准的 32 位 Windows 应用程序。

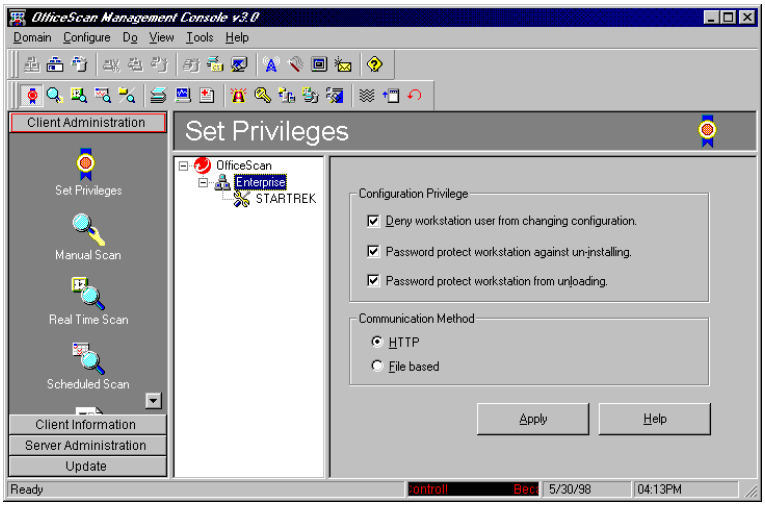

图 1: Windows 管理主控台

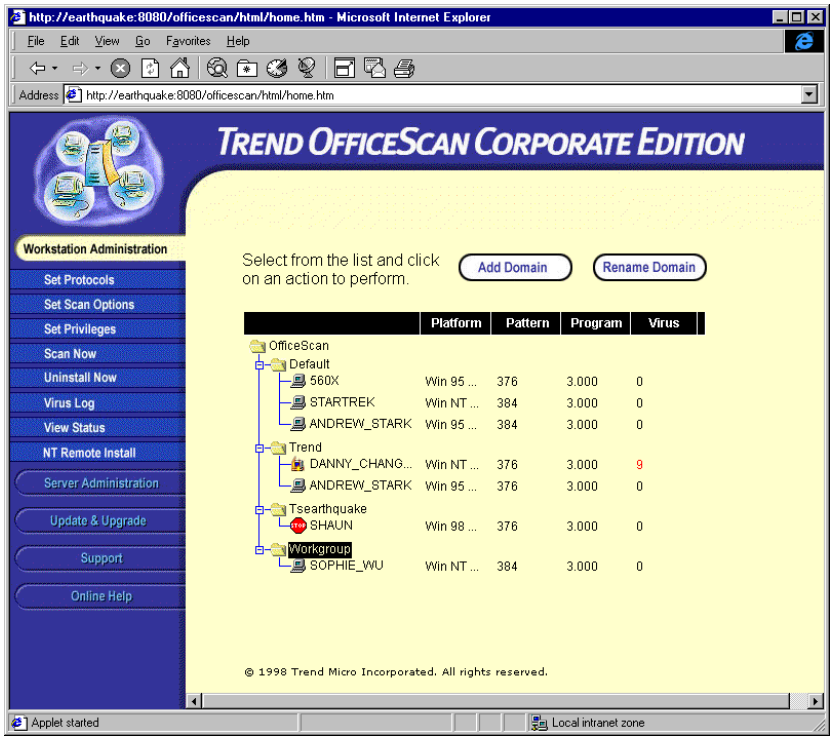

图 2: Web 管理主控台

二种 Office Scan 管理主控台皆提供下列功能， 让您管理企业网络的防毒策略：

客户端程序的完全控制

网络系统管理者可以透过管理主控台来控制客户端程序设定的每一部分，虽然客户端使用者可能被赋予设定本地端工作站扫瞄选项的权限，系统管理者仍然可以随时取消这些权限。

可扩充性

您可随时透过管理主控台安装或移除客户端程序来扩充或缩小 Office Scan 企业版 的网络。此外，Office Scan 经过特殊设计，可与趋势科技的其它企业防毒产品密切配合， 并且可与 Trend Virus Control System (Trend VCS) 整合。Trend Virus Control System (Trend VCS)是一项革命性的新型 web-based 防毒软件管理工具，安装的数套 Office Scan 可同时由一个 Trend VCS 主控台管理。透过单一且完整的主控台来管理数套安装于不同的网络环境或位置的防毒软件 已经不再是梦想。

完整的报告及客户端信息

Office Scan 管理主控台可显示您网络中所安装 Office Scan 客户端程序的完整的信息。病毒事件的记录文件储存于您网络中的服务器，并且可透过管理主控台存取。此外，系统管理者可管理客户端名称、产品版本、病毒码版本编号、操作系统、网域名称等重要的信息。

网域树状目录是 Windows 以及 Web-based 管理主控台的核心组件。此树状结构目录可显示了网络环境每一个 Office Scan 网域及安装的客户端程序。每一个客户端皆有一独特的图标显示其状态。客户端程序是否正常执行、是否感染病毒、或者客户端程序是否预先设定且未被移除等状态，皆可一目了然。

管理主控台还可以传送病毒警示通知至电子邮件或是呼叫器。标准的病毒警示告诉您网络环境中病毒事件的相关信息。严重中毒警讯则在病毒事件超越您所定义的临界点时通知您 (例如在

某段时间内发生某个数量的病毒事件)。既使系统管理者未使用管理主控台，警示功能随时会通知系统管理者有关网络环境的状态。

跨平台兼容性

Office Scan 企业版 提供了 Windows NT 与 95/98 版本的客户端程序。此外，Office Scan 管理主控台亦针对 Windows 3.1 及 DOS 版客户端程序提供了非主动式的支持。

其它特色

Office Scan 企业版当然具备了全功能防毒软件套件所应有的功能。

- **直觉式使用者操作接口**：管理主控台中大部分的功能可透过下列三种方式选取 – 菜单、工具列、以及 OfficeScan 功能区。
- **网域管理**：设定整个群组的计算机就如同设定一台计算机般简单。
- **远程扫瞄**：工作站的扫瞄可由管理主控台激活。
- **密码**：存取管理主控台及变更工作站客户端程序设定可由密码控制。
- **程序与病毒码档案更新**：更新的病毒码档案与程序组件可自趋势科技的网站下载，再部署至公司中所有的工作站。更新的动作亦可以预约执行的时间，依固定的时间间隔自动执行。
- **病毒码还原**： 若是病毒码档案造成任何病毒误判，可以还原为先前的版本。
- **紧急救援磁盘**：可为网络中每一台工作站建立紧急救援磁盘。您可以在感染开机病毒时利用这些救援磁盘重建硬盘的 MBR(Master Boot Record)。

Office Scan 客户端程序

Office Scan 企业版 包含工作站防毒软件，Office Scan 客户端可扫瞄安装此客户端软件的工作站是否有病毒存在，功能包括：

实时监控

实时扫瞄监控检查工作站存取的所有档案，病毒程序在档案被开启、复制或执行前就会被侦测到。任何含有病毒程序的档案，在该工作站中会出现一讯息窗口，且此事件会被记录在记录文件中，工作站使用者随后可检视此记录文件。此外，管理主控台可一并检视所有客户端程序的记录文件。实时监控可预防病毒感染安装客户端程序的工作站，建立网络环境中所有病毒事件事件的记录，并且还提供一个 CPU 活动监视表及关于所有预约扫瞄的信息。

手动 (On-demand) 扫瞄档案

工作站使用者可被指派扫瞄本地端计算机档案的权限。手动扫瞄是简单的程序，包含了二个步骤 – 只要在档案网域树状目录中选择要扫瞄的本地端磁盘驱动器，然后再按一个按钮即可。

预约扫瞄

您可以预约扫瞄执行的时间，频率为每日一次、每周一次、每月一次。

例外档案

您可选择不扫瞄的档案，在执行病毒扫瞄时略过这些档案。在极不可能的状况下，万一 Office Scan 客户端程序误判一未中毒的档案感染了病毒，您可设定扫瞄引擎略过这个档案。 若是包含了大型且复杂的宏文件或电子表格档案，在防毒软件扫瞄时无发正常运作，您也可以利用这个功能。

MacroTrap™ 科技防护宏病毒

最骇人听闻的计算机病毒讯息莫过于档案宏病毒的迅速扩散。许多文字处理软件及电子表格程序都提供了宏程序语言以进行自动化作业。这种语言亦可用来编写对计算机具破坏性的程序代码， 并且感染其它档案。自从 1995 年 7 月出现这种型态的病毒之后，Microsoft Word 档案为最常被感染的档案，但是 Microsoft Excel 与 Access 宏病毒也常出现。在 1997 年，仅仅一 只 Word.Concept 病毒就感染了二分之一的中大型企业与政府机关。目前被发现的中毒事件中，大约有百分之八十是各种型态的宏病毒。[2]

Office Scan 企业版 运用了趋势科技的 MacroTrap 科技，可在宏病毒档案散播之前，侦测到并清除这些病毒。

扫瞄压缩档案

压缩档案为透过电子邮件与 Internet 传输档案常用的方式，Office Scan 客户端程序可扫瞄 下列几种格式的压缩档案： arj、 binhex、 Cabinet、 compacked、 diet、 gzip、 lha、 lzexe、 lzh、 lzw、 mime、 MS compress、 pcaked、 pklite、 pkzip、 tar、 uuencode 、rar 等格式。您甚至可以扫瞄多重压缩的档案，亦即压缩于一压缩档案中的压缩档案。

多重的中毒档案处理方式

您可以设定客户端程序，在发现档案中毒时采取下列五种中毒档案处理行动：清除、隔离、删除、重新命名、不作处置。如果因为档案损毁(有时为计算机上的病毒造成)而无法清除病毒时，您还可以指定其它的处理方式。

其它方式的病毒防护

有效的企业网络环境防毒策略必须顾及四个层面，防护网络环境中病毒主要的入侵点：

- 工作站
- 服务器
- 电子邮件/群组软件
- Internet 网关器

趋势科技的 Office Scan 企业版 是一套主从式病毒防护解决方案，保护您公司的企业网络环境中每一台工作站。此产品还可趋势科技的其它防毒产品结合，例如 Trend ServerProtect、Trend ScanMail 及 Trend InterScan，为您公司的计算机网络环境提供一全面性的防护网。

[2] National Computer Security Association, Computer Virus Prevalence Survey, 1997