Panda Antivirus GateDefender

企业防病毒保护策略

技术白皮书

内容列表

企业防病毒保护策略

当前的问题

最近的数据指出，平均每204封电子邮件中就包含有一个病毒，并且99%的病毒通过SMTP邮件或HTTP网页浏览进入企业的网络环境。

而且，并不是只有病毒才会引起问题。2003年1月，蠕虫病毒SQL Slammer利用一个缓冲区溢出的漏洞攻击了全球数以千计的服务器，同时还在相当数量是SQL服务器上造成了拒绝服务攻击。根据Computer Economics的计算，该病毒造成的损失估计约有七亿零五百万欧元。

近几年来，计算机病毒利用的入口已经有了非常大的变化。以前，软盘和其他的可移动的装置是病毒传染的主要来源。而现在，Internet无疑成为了病毒传播的一个主要渠道。

同样地，从统计的数据上来看，经由Internet进入的病毒往往是：传播最为迅速并且非常危险的。由于时常采用多重的传播和感染方法，这些病毒被称为所谓的"混合威胁"。由于大部分的病毒经由电子邮件或Internet下载进入企业网络，因此在企业的网关上安装防病毒保护已经成为保证网络安全的一个基本要求。

然而，在企业的网络环境中往往存在着其他的病毒入口和传播途径，如：远程的膝上型电脑或通过调制解调器连接Internet、即时通信、基于Web的电子邮件或是使用POP3的外部邮件客户端，等等。由于这些多种多样的威胁以及未监控入口的存在，企业仍然会受到攻击。现在，Internet连接的安全性已经成为许多企业在制定自身网络安全策略时所优先考虑的内容。

根据Computer Economics所做的调查，99%的企业已经安装了各种类型的防病毒软件来进行保护。即便如此，76%的公司在去年仍然至少被一种病毒传染，有超过50%的公司则报告受到大量病毒的攻击。

或许你会简单地认为防病毒软件未能提供应有的适当保护。然而，事实却不尽相同。尽管99%的企业安装了各种类型的防病毒软件来进行防护，但往往会出现下面情况之一：

- 防病毒软件仅保护了某些特定的平台。在大部份的情况下，工作站和服务器属于被保护的范围，但并不是所有的企业都会为Internet与邮件网关服务器提供保护的

- 防病毒软件的设置不能有效地应付来自Internet的最新威胁，比如：桌面计算机系统上的永久病毒防护被禁用，防病毒软件版本过旧，松散的病毒库文件更新策略以及没有严格的网关内容过滤策略。

- 在许多公司里，一部分用户并没有应用防病毒软件策略。这或许是因为他们是远程的用户、系统管理员组或甚至仅仅就是因为没有设定策略。

下面的图表中显示了不同的病毒入口，传播途径以及对组织结构中各个层次的影响。

恶意程序的感染和传播途径

		企业的网络层次								
感染与传播途径		路由器/防火墙	代理服务器	SMTP网关与邮件中继	Web和数据服务器	应用程序和DDBB服务器	群件系统及协作平台服务器	文件服务器和储存区域网络	连接到网络的工作站	远程用户
电子邮件与信息	SMTP邮件中的恶意程序	☠	☠	☠			☠		☠	☠
	Webmail中的恶意程序	☠	☠						☠	☠
	POP3帐户中的恶意程序	☠	☠						☠	☠
	利用Outlook、Exchange的地址簿，通过电子邮件信息的方式传播蠕虫病毒	☠	☠	☠			☠		☠	☠
	利用即时通信、IRC、P2P等传播病毒与蠕虫。	☠	☠						☠	☠
安全漏洞	病毒和蠕虫利用软件的漏洞造成感染	☠	☠	☠	☠	☠	☠	☠	☠	☠
	过时或未被激活的防病毒软件保护	☠	☠	☠	☠	☠	☠	☠	☠	☠
Web浏览	隐藏于网页（ActiveX，Java...）中的恶意代码。...)	☠	☠		☠				☠	☠
	从Internet（HTTP/FTP）下载的恶意代码	☠	☠					☠	☠	☠
访问企业网络	通过网络共享传播的病毒和蠕虫	☠	☠					☠	☠	☠
	外部存储设备，如：软盘，CD-ROM，USB驱动器等。							☠	☠	☠
	被黑客安装的木马程序和后门程序	☠	☠	☠	☠	☠	☠	☠	☠	☠

层次化的防病毒保护策略

100%的绝对安全是不存在的。然而，熊猫软件公司将通过层次化的防病毒保护策略帮助您获得尽可能的安全环境。

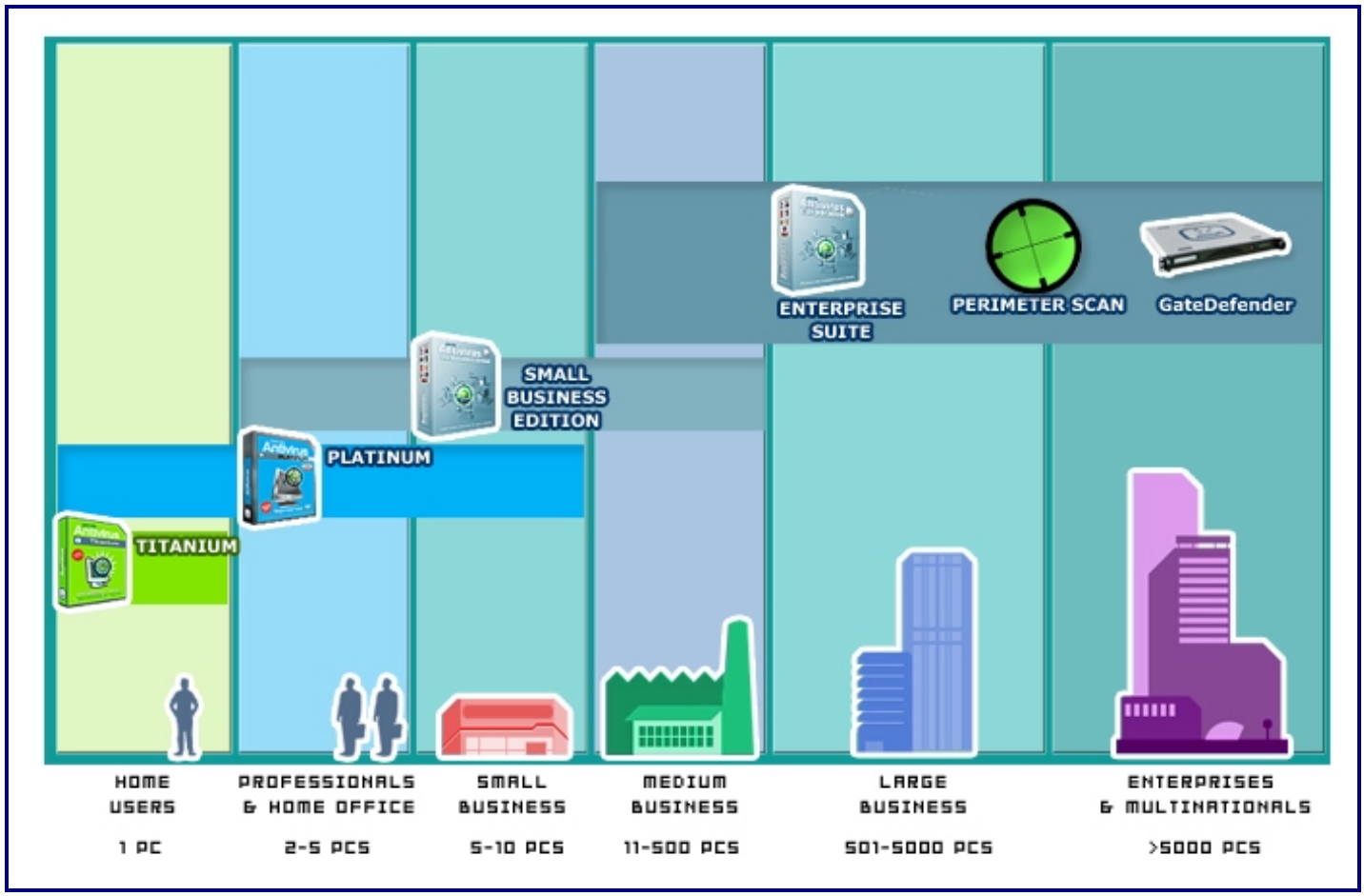
通过对组织结构中的所有层次提供防护-入境/出境的Internet连接（路由器），网页浏览（代理服务器，Web和数据库服务器），电子邮件网关（SMTP），数据储存（内部数据库服务器），内部信息系统（群件和协作），文件服务器和用户（桌面和远程用户）-，将能够对所有产品中所有可能的通信和信息交换协议进行防护。这样，网络的安全情况将开始接近我们盼望已久的100%安全。

基于这样的考虑，熊猫软件为组织结构中的每个层次都提供了一种不同的产品，并针对每个环境做了相应的优化（Panda Antivirus GateDefender主要针对Internet连接，PAV Exchange针对邮件服务器，铂金版针对桌面系统，等等）。

由于防护层次的增加，防病毒产品的保护效果也将变得更好。这种层次化的防病毒保护策略将使得病毒或其他恶意程序进入企业网络变得极其困难，这就大大降低了病毒感染与传播的危险性。企业网络中受保护的层次越多，防病毒产品的效率就越高，整个企业网络环境也就更接近于100%安全。

层次化的防病毒保护				
防病毒层次	描述	企业网络层次	保护对象	熊猫软件的产品
进/出Internet的流量	在病毒进入网络之前将其阻断。	· 防火墙 · 路由器	TCP/IP (SMTP, HTTP, POP3, FTP, ...)	· Panda Antivirus GateDefender · PerimeterScan防火墙版本 · PerimeterScan ISA服务器版本
网页浏览	阻断那些隐藏在Web页面中的病毒。	· 代理服务器	HTTP (files, Java Script, ActiveX)	· PerimeterScan 代理服务器版本 · PerimeterScan ISA服务器版本 · Panda Antivirus Integration Kit (API)
邮件网关	阻断隐藏在从Internet进入网络的电子邮件中的病毒。	· SMTP网关 · 邮件中继 · 邮件传输代理（MTA）	SMTP	· PerimeterScan Sendmail版本 · PerimeterScan Qmail版本 · PerimeterScan Postfix版本 · IMail服务器 (PAVCL) · 熊猫卫士防病毒软件Exchange模块 · 熊猫卫士防病毒软件Notes/Domino模块 · Panda Antivirus Integration Kit (API)
Web和数据库服务器	避免Web服务器受到病毒感染，阻止病毒向用户和客户端传播。	· Windows IIS 服务器 · MS SQL服务器	HTTP, 文件系统	· 熊猫卫士防病毒软件NT/2000/2003模块 · Panda Antivirus Integration Kit (API)
内部信息系统	阻止隐藏在信息，任务，公共文件夹中的病毒通过内部网络进行传播。	· 信息服务器 · 群件系统及协作平台服务器	MAPI, IMAP, SMTP	· 熊猫卫士防病毒软件Exchange模块 · 熊猫卫士防病毒软件Notes/Domino模块 · Panda Antivirus Integration for GroupWise (PAVCL)
文件服务器	阻止隐藏在文档，文件，程序中的病毒通过内部网络进行传播。	· 文件服务器 · 储存区域网络（SAN）	网络文件与共享，NetBIOS, SPX	· 熊猫卫士防病毒软件NT/2000/2003模块 · 熊猫卫士防病毒软件Novell NetWare模块 · Panda Antivirus Integration Kit (API) · 熊猫卫士防病毒软件命令行 (Win32/Linux)
对网络用户的保护	避免感染联网工作站上的用户。	· 连接到网络的工作站 · 被动式终端机 · Windows 98/NT/XP/2000	文件，协议，Webmail，POP3，MAPI，即时通信，光盘与软盘	· 熊猫卫士防病毒软件工作站模块 · 熊猫卫士防病毒软件铂金版 · Panda ActiveScan
对远程用户的保护	避免从网络外部造成的感染，并对网络中其他的病毒防护层次进行补充。	· 膝上型电脑 · PDA和移动电话 · 家中的个人计算机	文件，协议，Webmail，POP3，IM，光盘与软盘	· 熊猫卫士防病毒软件铂金版 · 熊猫卫士防病毒软件钛金版 · Panda ActiveScan

下面的图中显示了针对各种类型用户各个层次推荐的不同防病毒解决方案。每种解决方案都具有自己的特性，防病毒程序与反恶意程序产品能够为每个层次提供符合需求的通信协议保护及相应的良好性能。



Panda Antivirus GateDefender：层次化的安全

"我们有相当多的理由来选择安装Panda Antivirus GateDefender：它拥有完整的病毒检测和内容过滤报告，用户可定制的警告和通知，它甚至还包含了对扫描引擎更新可能的提醒。仅仅利用一个简单而且能够持续自动刷新的监视系统，管理员能够非常方便地对统计到的网络数据流量以及Panda Antivirus GateDefender对恶意程序的检测结果进行完全访问。"

Nireo公司的IT系统主管

Panda Antivirus GateDefender是一款集成了硬件和软件的高性能专用防病毒服务器，并且它被设计为'连接后即可遗忘'。它能够在所有的病毒，蠕虫和其他恶意程序进入企业网络之前将它们阻断。

由于高扩展性和负载均衡能力，它能够满足小型，中型以及大型企业的需求，透明地调整网络数据流量。

	Panda Antivirus GateDefender 7100	Panda Antivirus GateDefender 7200
目标企业（用户）	500用户及以下	超过500用户
硬件特性	Pentium III	Dual P4 Xeon
内建负载均衡	是	是
内嵌操作系统	Windows NT	Windows XP
每小时扫描电子邮件数量	80,000	200,000
以太网接口	10/100	Gigabit 10/100/1000

抵御病毒的第一线

平均每204封电子邮件中就包含有一个病毒。

作为第一款能够为七种常用通讯协议提供保护的网络边界防病毒解决方案，Panda Antivirus GateDefender能够对使用SMTP，HTTP，POP3，FTP，NNTP，IMAP4和SOCKS协议进出网络的数据通讯提供防病毒保护，而这一点是市场上同类型的网络边界防毒产品所无法做到的。

同样地，Panda Antivirus GateDefender还将解放企业网络中的服务器，让它们能够专注于自己的首要任务（文件服务，邮件路由，信息及其他）。由于病毒在能够进入到企业网络之前就已经被阻断，因此这些服务器将不再需要进行扫描以及内容过滤。

连接后即可遗忘

与针对桌面计算机与服务器的传统防病毒保护需要人工干涉（扫描引擎的更新，配置等）的情况不同，Panda Antivirus GateDefender的工作是完全自动且透明的。也就是说它可以完全独立地自行运作。

不论是小型公司还是大型企业，Panda Antivirus GateDefender都同样能够适用，它对于网络的数据流量是透明的。它的保护系统被设计为在任何的网络中都能简单地实现，而并不需要复杂的设定调整或是改变网络的数据流量。

所有使用最广泛的通讯协议都受到保护，并且它的内容过滤功能可以阻止未知的病毒和蠕虫进入企业网络。

安装Panda Antivirus GateDefender应该只需花费三十分钟左右的时间。并且，在安装完成之后不需要专门的人员来对它进行管理。

最少的管理需求

能够利用一个简单的Web控制台对Panda Antivirus GateDefender进行安全的远程管理，并且根据默认设置它会持续的完成自动更新。Panda Antivirus GateDefender每天至少更新一次。当有病毒警告（比如由Bugbear.B引起的病毒事件）时，病毒库文件将每半小时更新一次以避免任何与该病毒有关的事件产生警告。

Panda Antivirus GateDefender还提供关于检测到的病毒以及网络数据流量的警告信息和报告，同时还包括了每年365天每天24小时的电话与电子邮件技术支持。

层次化的企业安全防护

百分百的绝对安全是不存在的。然而，熊猫软件公司将通过层次化的防病毒保护策略帮助您获得尽可能的安全环境。并针对每个层次的不同环境做了相应的优化（Panda Antivirus GateDefender主要针对Internet连接，PAV Exchange针对邮件服务器，铂金版针对桌面系统，等等）。

Panda Antivirus GateDefender以一个额外安全层次的形式出现在企业的网络安全环境中。由于它能够阻止蠕虫，病毒和木马程序进入网络，因而能够为已安装的其他类型防病毒产品提供完美的补充。

工作站上防病毒软件能阻止那些利用膝上型电脑，Webmail，外部POP3账户或即时通信程序进入企业网络环境的病毒造成破坏。同样地，Panda Antivirus GateDefender能够阻止病毒通过Internet进入（或离开）企业网络，同时它还能阻止类似于SQL Slammer这种利用系统漏洞进行攻击而传统防病毒软件又无法加以抑制的病毒。

如果企业内部并没有建立起防病毒保护，那么在病毒通过某种途径（例如通过膝上型电脑）进入到网络之后，Panda Antivirus GateDefender将只能够阻止该病毒从企业网络离开，但整个企业的内部网络仍然会受到感染--服务器和工作站将可能会崩溃，网络管理员将不得不把精力花费在对整个系统的病毒清除上。

同样地，如果仅仅对工作站、文件服务器和邮件服务器提供防毒保护，企业内部网络仍然会遭到诸如LoveLetter，Klez，Nimda和SQL Slammer这类病毒的攻击。它们将导致服务器崩溃，引发拒绝服务攻击或只是迫使系统管理员关闭系统以避免进一步传染的潜在威胁。

由于Panda Antivirus GateDefender能够帮助提升性能并阻止病毒利用与防火墙集成的传统防病毒软件不能发现的安全漏洞，因此它还能作为对防火墙集成防病毒软件的一个有效的补充。Panda Antivirus GateDefender是专注于防病毒功能的服务器，而防火墙则是专注于访问控制的服务器。这种功能上的分离应该是企业对内部主要服务器进行设置时所应遵循的一项基本原则。

显而易见的，熊猫软件公司提供的层次化安全防护策略能帮助您努力实现100%的网络安全。每个增加的保护层次都将使您在整个网络中已有安全解决方案的价值呈指数地增长。

层次化的边界防护

SAPO门户网站是第一个在葡萄牙为140万用户提供病毒防护的Web邮件系统供应商。Panda Antivirus GateDefender每天为该门户网站的用户所收发的超过1百万封邮件和邮件附件提供病毒扫描和防护。该病毒防护方案所提供的高效率和高性能是两家公司达成协议的原因。"与熊猫软件公司达成协议是整个冗长的技术和战略决策过程的关键和和亮点，它对于确保SAPO的产品在葡萄牙市场上保持领先地位非常重要。在整个过程中，熊猫软件公司所表现出来的技术能力起到了一锤定音的作用，这要归功于他们所提供的高级别的病毒防护和熊猫软件公司在葡萄牙的专业团队的灵活性和高效率。"

José Carlos Baldino, SAPO产品总监

Panda Antivirus GateDefender是一个可以兼容于Panda Antivirus Enterprise Suit的额外的边界病毒防系统。Panda Antivirus GateDefender并不会用于替代Panda Antivirus Enterprise Suit，因为它们适用于不同的环境：Panda Antivirus GateDefender用于保护网络边界通讯，而Panda Antivirus Enterprise Suit用于防护网络内部的工作站和服务器。

尽管熊猫的另一个产品Panda PerimeterScan包含了一系列专用于边界网关服务器（如：Sendmail、Firewall-1、Proxy、ISA、Postfix、Qmai等）的病毒防护软件，但Panda Antivirus GateDefender提供了一个高性能、易使用的完整解决方案，它可以更好地符合绝大部分企业的需求：易于安装和管理。

仍然可能存在这种情况，由于Panda Antivirus GateDefender不包含一些特殊的防毒防护功能，网络管理员依然倾向于使用基于Panda PerimeterScan的软件来防护边界网关服务器，比如Firewall-1或Sendmail服务器。下表列举了一些Panda Antivirus GateDefender和Panda PerimeterScan适用的情况：

功能或特性	PAV GateDefender	PerimeterScan
网关级网络边界防护	√	√
保护任何计算平台和网络结构（Unix, Solaris, 等等）	√	
Sendmail, Qmail, Postfix, ISA, Proxy or Firewall-1 with Win32 或 Linux	√	√
Sendmail, Qmail, Postfix, ISA, Proxy or Firewall-1 with Unix, Solaris, HP-UX 或其他 Unix	√	
与网关服务器软件直接集成		√
需要高级的病毒防护功能		√
需要高级的内容过滤功能	√	
保护IIS、SQL和Outlook的系统漏洞	√	
企业中有专业的IT人员	√	√
企业中没有专业的IT人员	√	

技术信息

"该系统自动更新病毒特征码定义文件和病毒扫描引擎，以确保其始终能够有能力应对最新的威胁。"

Byte杂志．推荐产品

主要特点

管理配置	直观的Web界面(HTTP)
网络集成	可以设置为一个单独的网桥，无需另外的代理服务器和防火墙。 Panda Antivirus GateDefender需要一个IP地址和名称。
病毒特征码定义文件和扫描引擎更新	自动实现，无需人工干预
支持的协议	进出网络的以下所有协议都会被扫描：HTTP（包括Java和ActiveX），FTP，SMTP，POP3，IMAP4，SOCKS和NNTP
传输能力	GateDefender 7100：最大12Mbps GateDefender 7200：最大30Mbps
容错性	多级别Watchdog监控系统
防病毒动作	自动破坏染毒文件
报告和警报	在防病毒动作中可自定义警报和报告（发现病毒、更新、其它事件等）
网络接口	GateDefender 7100：10/100百兆以太网接口，RJ-45 GateDefender 7200：10/100/1000 千兆以太网接口，RJ-45
尺寸(长 x 宽 x 高)	机架式 GateDefender 7100：Mini 1U (16,7" x 1.75" x 14") GateDefender 7200：标准 1U (19" x 1.75" x 20")
电源	自动检测，110V/60Hz或220V/50Hz，最大200W
认证	FFC和CE认证

Panda Antivirus GateDefender 7100	Panda Antivirus GateDefender 7200
· 样式 - Mini 1U 机架式 · Pentium III 1.26 GHz · HD 40 GB · 512 MB RAM · LAN 2×10/100 Mbps	· 样式 - 标准 1U 机架式 · 双Xeon 2.4 GHz 512K - 533MHz · HD 40 GB · 1 GB DDR RAM · LAN 2×千兆 NIC

软件特性

协议侦听和防病毒配置

Panda Antivirus GateDefender有两个基本的模块组成，一个是协议侦听模块，一个是病毒扫描模块。这使得它成为了唯一可以防护所有最常用的网络应用协议（SMTP，HTTP，POP3，FTP，NNTP，IMAP4和SOCKS）的边界病毒防护解决方案。Panda Antivirus GateDefender侦听并检查使用上述协议进行数据传输的数据包，将它们通过内存传递给病毒扫描引擎，而无需将数据写入硬盘。这样，它就可以检测到其他防病毒产品无法检测到的恶意代码（如SQL Slammer，WebDAV，等等）。

一个Panda Antivirus GateDefender 7100设备可以每小时最多扫描80,000封邮件，其中25%的邮件被病毒感染。上述功能的完成是完全透明的。Panda Antivirus GateDefender物理上通常位于防火墙和局域网之间。所有通过Panda Antivirus GateDefender的数据都会自动进行病毒扫描，且不会干涉正常的Internet访问或消耗过多的带宽。

Panda Antivirus GateDefender可以识别和扫描下列格式的压缩文件：

ZIP，GZIP，ARJ，LHA，RAR，ACE，InstallShield CAB，Microsoft CAB，Microsoft COMPRESS，TAR，QUAKE，MIME UUEncoded，MIMEXXEncode，MIME BinHex，RTF，PDF，ZOO，FREEZE，BZIP2，COMPRESS，ARC，和 LZOP。

下列可执行文件加壳程序的格式同样可被识别和扫描：
LZEXE，PKLITE，ICECOM，DIET，UPX，CRYPTCOM，AS-PACK，PE-PACK，PELite (1.2，1.3，1.4/2，1/2.2)，PKLITE32，WWPack32，Crunch v1，PE-Protect，FSG 和 TeLock。

操作系统

Panda Antivirus GateDefender运行嵌入式Windows操作系统（单处理器的7100使用NT，双处理器的7200使用特别优化的XP）。上述操作系统都经过特别强化而不包含任何系统漏洞。众所周知，任何操作系统的安全性只与其配置相关，所以Panda Antivirus GateDefender仅在上述操作系统中运行必要的服务，以使其可正常工作，从而最大限度的封杀了遭受恶意代码攻击的可能性。

运行于Panda Antivirus GateDefender中的操作系统仅包含了使Panda Antivirus GateDefender正常工作的服务和进程并只对外部开放了2个端口，它们是对其进行管理所必需的。

TCP/IP的开放端口分析

Panda Antivirus GateDefender作为一个透明的网桥位于Internet和企业的内部网络之间。这意味着所有经过Panda Antivirus GateDefender的网络数据都将被侦听且那些被配置为需要扫描的协议数据将被扫描，而这一切都是完全透明和自动的。

由于使用了上述机制，Panda Antivirus GateDefender不需要开放任何的TCP/IP端口或者说不需要在任何的TCP/IP端口进行监听来达到进行病毒扫描的目的。实际上，Panda Antivirus GateDefender仅开放了2个TCP/IP端口，它们用于管理目的。端口80用于接受对Web控制台的访问，用于日常管理。端口5900则用于在用户需要时进行故障诊断。建议用户在通常情况下阻断对Panda Antivirus GateDefender端口5900的访问，除非您需要熊猫软件公司的技术人员连接到该端口来协助您进行故障诊断。

在对Panda Antivirus GateDefender进行端口扫描时，非常重要的是请记住请使用单台电脑使用交叉线与Panda Antivirus GateDefender单独相连，因为如果Panda Antivirus GateDefender连接在网络中的话可能会产生错误的结果。如果在Panda Antivirus GateDefender后存在一台服务器的情况下进行端口扫描的话，得到的结果可能是该服务器上的开放端口而不是Panda Antivirus GateDefender上的。

对管理控制台IP地址的端口扫描

该IP地址用于访问内部的管理Web服务器；出厂的缺省设置为1.1.1.5。在该IP地址上唯一开放的端口为80，内部的Web服务器通过它接受对Web管理控制台的管理界面的访问。

对GateDefender IP地址的端口扫描

如果GateDefender的IP地址为172.16.1.244，唯一开放的端口为VNC端口，比如端口5900。就如上面所提到的，建议通常情况下在防火墙上阻断对该端口的访问。

对IP地址1.1.0.2的端口扫描

在该IP地址上无任何开放的端口。

对IP地址1.1.0.6的端口扫描

在该IP地址上无任何开放的端口。

容错系统

" Panda Antivirus Appliance的部署大大提升了Europa Press IT系统的安全性。在使用了Panda Antivirus Appliance之后，我们原有的Internet应用在不受任何性能影响的前提下变得更加的安全与可靠。同时，这也意味着我们有理由确信没有病毒能够感染我们的系统，各代理机构的客户端也不会从我们这感染到病毒。"

Europa Press的IT主管

Panda Antivirus GateDefender简单而有效的"连接后即可遗忘" 设计使您的管理需求降至最低。它还具备了一系列诸如WatchDog或Master Boot Manager之类的自动修复工具，以防止长时间的网络连接故障。

传统意义上的容错指的是创建一个所谓的"子系统"，该系统和原有系统处于平行运行状态，用来提供的额外的运作能力。而在这里，容错被定义为一个后备系统以确保相关服务的连贯性。

Panda Antivirus GateDefender具备多重容错系统，以保证这款边界防病毒产品的的可靠性。这些系统的设计用途是在下列组件中的任何部分出现故障时对系统进行恢复：

- 硬件：主引导记录或硬盘故障
- 防病毒软件：病毒扫描引擎及服务故障
- 协议侦听：TCP/IP数据包侦听服务故障
- 操作系统：操作系统故障

Panda Antivirus GateDefender拥有的主要容错系统是WatchDog和Master Boot Manager。

WatchDog

WatchDog系统是通过Panda Antivirus GateDefender主板上设计的一个系统监控电路来实现的。

它的功能从本质上来看是简单的。WatchDog会每隔10秒钟对Panda Antivirus GateDefender设备状况进行检查，如果没有得到相应的正确响应，WatchDog将通过主板上的设备重新启动系统。

由于建立了这种容错系统，Panda Antivirus GateDefender能够在具体应用或是操作系统本身出现故障时自动进行系统恢复。

Master Boot Manager

某些极端的环境（如高温等）很有可能会对Panda Antivirus GateDefender的硬件造成损害，比如说硬盘或者是主引导记录出现损坏。

为了避免上述情况导致系统产生故障，并且确保边界防病毒服务能够持续有效地正常运行，Panda Antivirus GateDefender中包含了一个名为Master Boot Manager的专用工具。该工具由汇编语言编写而成，其设计目的是使操作系统具有自动故障恢复和自我修复的功能。

Master Boot Manager系统位于硬盘的起始部位。同时，在硬盘上主分区之外的位置还物理保存了多个隐含的主分区拷贝。

当Panda Antivirus GateDefender启动时，Master Boot Manager系统将依据上一次正常启动的结果检测当前应该被用于启动系统的分区。

如果Master Boot Manager发现主引导分区因为某种原因发生了故障。它将使用一个现有的拷贝修复损坏的分区，并从一个正常的分区引导系统。

与此同时，Master Boot Manager将清除被损坏的分区并尝试修复它，以确保它们在以后的系统启动中恢复正常的功能。

注意：目前还有其他的一些网络边界安全解决方案宣称通过使用SCSI RAID磁盘系统来保证系统的高可靠性。熊猫软件认为：SCSI RAID磁盘系统只有在类似于存储服务器这类需要实现数据保护和提供高可靠性的应用时才是不可或缺的要素。然而，SCSI RAID磁盘系统并不能为那些无需进行高可靠数据存储的设备带来更多的好处，比如Panda Antivirus GateDefender以及市场上其他一些同类型的硬件网关防病毒产品。然而这是一个完全不同的市场需求，这样的磁盘系统为最终用户带来的仅仅只是成本的增加，熊猫软件非常乐意为用户节省这些不必要的开销。Panda Antivirus GateDefender使用象WatchDog和 Master Boot Manager这样的工具来为用户提供高可靠性和负载均衡能力。

内建的负载均衡

"促使我们购买Panda Antivirus GateDefender的原因是：它的透明性、配置简单以及运行速度快。这款产品为我们提供了简单的资源管理手段和轻松的工作环境。"

IKT的总经理

在高可靠性之后，对于边界防病毒服务器而言另一个重要的方面是数据处理能力的扩展性。

在建立高可靠性系统或服务的过程中，很多公司一般都不会在意网络带宽的平均占用率，而是更关心数据流量的峰值。因为正是在这种临界状况下系统最容易发生过载、故障和崩溃。

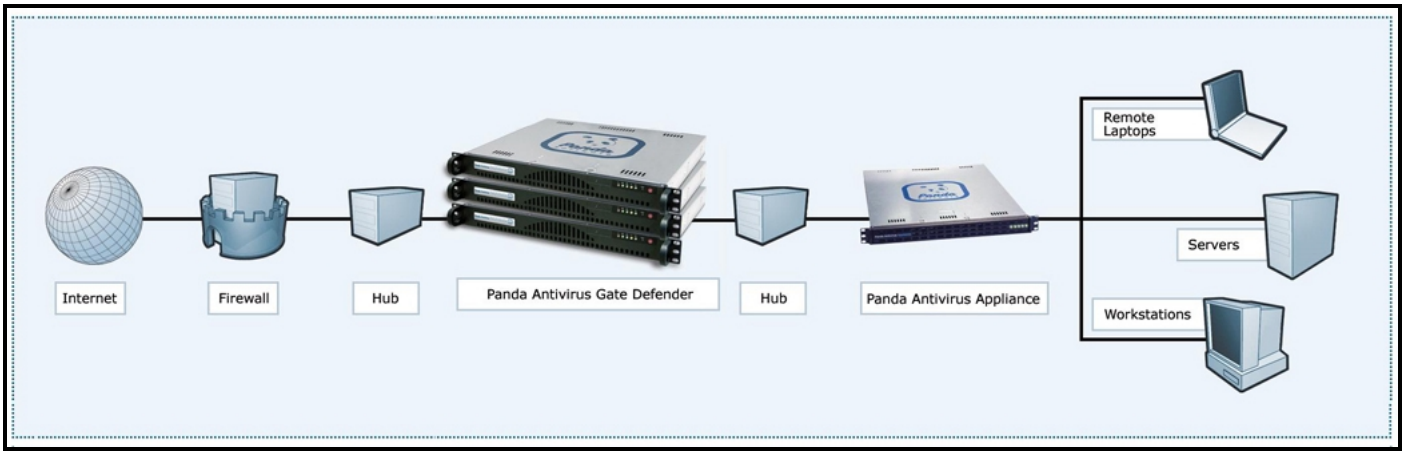
由于设计时考虑到网络边界防病毒产品在对大量数据进行扫描时必须具备足够的扩展能力，Panda Antivirus GateDefender中包含了内建的负载均衡系统。

同样，如果一台Panda Antivirus GateDefender设备停止工作，其他的Panda Antivirus GateDefender设备将在几秒中内自动接管发生故障的设备所承担的工作量。

这种负载均衡的能力有益于保证网络数据传输的畅通。在Panda Antivirus GateDefender对网络通信影响已经降到最低状态（大约3%）的情况下，通过负载均衡的解决方案可以进一步提升数据扫描的速率和连接速度。

负载均衡的技术细节

当两台或两台以上的Panda Antivirus GateDefende设备被安装在同一个网段内之后，负载均衡的功能将在很短的时间之内自动开始工作。当然，这些设备必须能够'相互发现'，比如：处于同一网段内的两个集线器之间，如下图所示：



当处于相同网段内的多个Panda Antivirus GateDefender设备准备实现负载均衡功能时，它们中的一个将被标识为主控机。从这一刻起，即使所有的Panda Antivirus GateDefender系统都能够"看见"通过该网段的数据，Panda Antivirus GateDefender系统还是会利用随机的算法来确定每台设备所应负责扫描的用户会话。这些决定是基于每个会话单独的源和目标IP地址所做出的。

注意：在两个交换机而不是集线器之间的多台Panda Antivirus GateDefenders设备上实现负载均衡是可行的。此时，交换机上所有与Panda Antivirus GateDefenders设备连接的端口必须被配置成广播模式。

启用负载均衡功能的设备彼此之间会保持连续的通信，它们将能够自动判断当前工作设备的数量以及正在启用负载均衡功能设备的数量。如果一个设备因为某种原因而出现故障，剩余的设备将在所有可用设备中对通信流量进行重新分配。此时，剩余的设备将花费22秒的时间来取得对故障设备所承担网络数据流量的控制。当出现故障的设备重新开始工作时，新的负载均衡的建立将在12秒之内完成。

同样的，这些设备间会进行频繁的通信来检查它们是否使用相同的随机算法，以确保网络通信负载能够被正确地分配。

传输速率分析

根据对导致网络传输冲突的考虑，我们可以设想以太网络实际性能的极限大约是其理论值的70%。那么，对于100Mbps的网络而言，在两个集线器之间实现负载均衡的多个Panda Antivirus GateDefender设备所能实现的最大传输吞吐量大约是70Mbps。

Panda Antivirus GateDefender负载均衡群集的数据扫描速度实际上是由每一个设备所忽略的无需扫描的数据包计算得出。这种采用数据包数量而不是真正的网络带宽通信量的算法定义是有局限性的。比如，当网络中出现大量的小容量数据包时，Panda Antivirus GateDefender将可能达到其性能的极限，虽然此时很有可能真正的网络传输量实际上很小，网络带宽资源占用也很低。

目前市场上也有采用'共享'负荷的方法来取代负载均衡的解决方案。NAI研发的WebShield e500和e1000就属于这种情况。此类解决方案在安装用来扩展性能的设备以满足实际应用中对扫描带宽的要求时，必须增加一个额外的组件来实现不同设备之间的负载分配。在这种情况下，由于需要扫描的数据必须在担任负载均衡的额外组件与防病毒设备之间来回往返，也就意味着整个数据扫描的带宽将被分为两个部分。

在性能上，Panda Antivirus GateDefender每秒钟可以完成对19个电子邮件信息的扫描，其中假定所有电子邮件信息都没有受到病毒的感染。两台Panda Antivirus GateDefender设备每秒钟可以完成对35个以上电子邮件信息的扫描（大约是每秒钟100 KB）。

抵御漏洞

"对于我们而言，最重要的是在浏览Internet的时候抵御病毒。前几天，在未造成网络瘫痪也无需管理员做任何操作的情况下，它成功地阻止了Bugbear.B的入侵。"

FiestaCandy的IT经理

正如先前所提到的，Panda Antivirus GateDefender既能阻止病毒进入企业，也能阻止病毒从企业网络中向外传播。

而且，Panda Antivirus GateDefender也能够阻止那些利用不同安全漏洞为企业内各部门带来破坏的恶意企图。

抵御MIME报头漏洞

这个MIME报头漏洞，会对Outlook与Outlook Express的5.01和5.5版本造成影响。该漏洞将允许邮件附件中的内容在用户阅读这封邮件（甚至没有打开附件）时自动运行。而这些文件附件的内容将可以是病毒，蠕虫，木马程序等。

MIME是一个为接收和发送综合内容（执行程序，语音文件，图像文件等）而开发的协议。MIME根据类型分类消息中的内容并且添加两个标识（MIME-Version和Content-type），其中后者指定了消息代码内容所属的分类组。

对这些标记的修改将会导致Internet Explorer错误地把一个执行文件当成影音文件和图像文件来处理。Klez，Bugbear.B，Nimda，Badtrans或Frethem仅仅是许许多多利用了该漏洞的病毒中的一些典型代表。

当发现MIME类型与其文件扩展名不相符时，Panda Antivirus GateDefender便能够确认该电子邮件报头已经被修改并能利用安全漏洞。这样，即便电子邮件的阅读者受到此安全漏洞的影响，附件文件也不能自动运行。

抵御其他非常规的报头漏洞

Panda Antivirus GateDefender也能够抵御其他影响系统的漏洞，包括如下：

VBS 附件漏洞：这个漏洞允许电子邮件消息中的VBS代码被当成HTML代码而自动运行。Panda Antivirus GateDefender通过它的文件过滤功能，能够阻止潜在的危险文件，其中就包括那些扩展名为VBS的文件。

CLSID 扩展名漏洞：能够隐藏附件文件的真实扩展名。Panda Antivirus GateDefender能够阻止带CLSID扩展名的文件。

非标准文件扩展名漏洞：MIME报头指定诸如文件的主题、数据或名字的数据。过去，有过通过数据和文件名字使Outlook Express缓存溢出的漏洞。通过使用特定的过长字符串，一个老练的攻击者能够在受到攻击的计算机上运行代码。这些漏洞有时被利用来洞察远端网络或插入病毒、蠕虫。为了避免利用这种类型的漏洞攻击，Panda Antivirus GateDefender将阻止用文件名以点(.)结尾的文件。

抵御IIS 5.0 WebDAV漏洞

WebDAV (World Wide Web Distributed Authoring and Versioning)是一个HTTP1.1版本协议的扩展名。这个协议提供一个通过Internet进行编辑和管理操作的标准。WebDAV在Internet Information Server 5.0中是一个默认组件，允许通过HTTP连接进行文件的写，复制，删除，编辑等操作。

然而，已经发现了一个由不检测缓存造成的漏洞。该漏洞可以被远程利用以进行拒绝服务攻击或获取对整个机构控制。

更准确的说，在这种情况下当向Internet Information Server发送请求的HTTP报头中包含的URL超过了65KB（超过50000字符）就将导致缓存溢出。

近期的研究显示，超过四分之三的Microsoft IIS 5.0服务器启用了WebDAV组件，这也就意味着有超过6百万的Web站点存在有该漏洞。

Panda Antivirus GateDefender在TCP/IP层面进行检测，阻断可疑文件的同时避免安全漏洞被利用。Panda Software的边界解决方案已经被设计为阻断任何超过40KB的HTTP报头。

尽管Panda Antivirus GateDefender能够帮助企业抵御诸如此类的漏洞，但仍然推荐安装Microsoft所发布的针对该漏洞的IIS 5.0修复补丁。

抵御SQLSlammer和类似蠕虫

2003年一月， SQLSlammer通过利用服务器缓存溢出漏洞攻击了全球数千台SQL服务器，Computer Economics估计经济损失7亿零5百万欧元。

SQL Slammer利用拒绝服务攻击(DoS)通过1434端口发送大量包含蠕虫的数据包来攻击服务器。它的功能和特征类似于红色代码（Code Red），红色代码利用IIS服务器的.ida漏洞能够在脱离传统存储设备的情况下迅速进行传播。

Panda Antivirus GateDefender 在TCP/IP层面进行扫描，阻断那些试图利用SQL服务器上已知漏洞的数据包。事实上它能够阻止对Microsoft在其安全公告牌上公布的两个缓存溢出和一个拒绝服务 (DoS)漏洞的利用企图。这意味着它能够阻止任何SQLSlammer类型的攻击。

即使Panda Antivirus GateDefender能够有效地实时抵御SQLSlammer，但仍然推荐安装Microsoft所发布的修复SQL服务器中漏洞的补丁。

抵御双扩展名的文件

大量的病毒、蠕虫或木马程序 (Klez.I, Bugbear.B, 等)为了不引起邮件读者的注意而使用双扩展名进行传播。因为邮件读者通常只显示附件一个扩展名甚至不显示扩展名。

Panda Antivirus GateDefender通过阻断所有超过一个扩展名的文件来保护企业免受此类问题的困扰。

尽管这种设定能够为企业提供额外的安全防护, 您也可以在Panda Antivirus GateDefender的管理控制台中使用'Don't scan files with the following extensions'来禁用此操作。

例如, 如果您不希望对REPORT.V3.DOC.TXT文件进行扫描, 可以在Panda Antivirus GateDefender中的扫描设置中选择排除所有的TXT文件。

Panda Antivirus GateDefender

企业防病毒保护策略

技术白皮书