终端安全

基础指导手册

终端安全基础指导手册

企业数据泄漏的事件从未停止过。很多人感叹黑客太厉害了，但这只是众多企业遭受攻击的部分原因。事实上，大多是企业被黑都是因为他们自己的安全保护太简单，太疏忽了。为什么我们有了越来越多先进的安全技术，但遭受攻击的次数却有增无减呢？

之所以形成这样的趋势，很重要的一个原因就是企业终端上的安全事件不断增加。美国安全专家 Mark S.Kadrich 在其《终端安全》一书中曾表示，终端安全是影响信息系统安全的根源，应通过确保终端安全进而确保网络安全。

本技术手册将分几部分，为你提供保护常见终端安全的技巧和方法，降低你数据泄漏的风险。

定义终端安全

终端安全从提出到现在，在概念上已经经历了很大的变化，从最初是指安装在电脑上的反病毒软件，到后来的包括台式机、笔记本电脑、移动设备的安全防护，再到以网络为中心的访问控制管理，强调所有联网设备的安全，符合企业安全策略所定制的标准，保护网络免受病毒、木马的侵害。美国顶级的安全专家 Mark S.Kadrich 在其《终端安全》一书中就明确指出，终端安全是影响信息系统安全的根源。

本部分中，我们将为你定义终端，带你了解终端安全的现状及面临的挑战。

- ❖网管思考　终端安全能否代表全网安全
- ❖你是否忽视了终端安全？

终端安全之服务器安全

随着 IT 技术的革新，各种病毒层出不穷，黑客们的花招也越来越多。而处于互联网这个相对开放环境中的服务器遭受的风险比以前更大了。越来越多的服务器攻击、服务器安全漏洞，以及商业间谍隐患时刻威胁着服务器安全。服务器的安全问题越来越受到关注。我们要如何保障服务器的安全呢？

- ❖你的 Windows 服务器得到适当保护了吗？
- ❖Windows 服务器补丁你伤不起！
- ❖Linux 服务器系统最佳安全实践

终端安全之移动设备安全

移动设备的趋势已是必然，随处可见的智能手机，平板电脑都在向我们显示这点。移动设备在为用户带来好处的同时，也带来了潜在的威胁。如何保证移动终端的安全？本部分我们将为你提供一些策略和方法。

- ❖移动设备网络防御战略
- ❖针对企业 iPad 终端整合的安全策略
- ❖移动设备：企业安全策略
- ❖保证移动办公用户的安全
- ❖建立安全策略应对移动设备威胁

制定完整的终端安全策略

今天的安全威胁正日益变得花样百出，而经济利益的驱使，又使得这些威胁越来越多地趋于隐藏自己，这些无孔不入的安全威胁对企业业务造成的安全挑战，在终端领域表现得淋漓尽致。终端安全需要一套完整的安全防护，只是单纯的在每个终端上不断更换性能更快、更高的安全设备是远远不够的。

- ❖制定网络终端安全政策　防御恶意攻击
- ❖终端数据丢失防护部署中的五大安全技巧
- ❖怎样箍紧终端安全的“木桶”

网管思考　终端安全能否代表全网安全

网络病毒、新型的 DoS 攻击、间谍软件、木马、网络钓鱼陷阱及黑客入侵等愈演愈烈，仅仅靠“堵漏洞、设高墙、防外攻”的过去防护策略，已经无法保证现在的网络安全。而终端的安全性问题也日渐突出，根据目前的网络现状，如果终端安全受到威胁，即使网络中的核心设备安然无恙，整个网络的业务运行也会受到严重影响甚至瘫痪。建设一个有效的终端安全管理体系，不仅能够保障终端安全，而且能够提升网络整体的安全防御能力。

终端的概念

终端到底是什么?在目前的信息安全领域，终端一般指网络中的一台可能由任何人操作的一台计算机，事实上，服务器也可以归结为广义上的终端。终端由于应用和使用的复杂性，目前没有关于终端安全详细的描述与定义。可以说，影响计算机使用者正常处理和完成职务工作的计算机软件、硬件使用，以及违反公司信息系统和行政管理规定的计算机应用，均可认为是触发了终端安全或终端管理事件。

终端安全现状

过分相信网关安全。在网关安全方面，认为安装了防火墙、入侵检测系统等网络就安全了。现在终端安全出现严重问题，包括:安全保护问题、系统管理问题和行为监控问题。其中安全保护问题包括：病毒蠕虫大规模泛滥以及新的蠕虫不断出现给用户带来损失;来自内部和外部的入侵和攻击的问题;网络边界扩展带来的对于移动办公用户、第三方接入安全防范不足从而引入安全风险的问题。而系统管理问题则主要表现在对微软等操作系统不断出现漏洞的补丁措施的及时管理，以及网络中终端设备资产信息变化的精确统计管理问题。至于行为监控，则是企业主对于员工的安全监控预防和工作情况统计的措施。

如何解决终端安全

从目前的终端安全和终端管理技术上来看，网络的终端安全管理主要是从终端状态、行为、事件方面来进行防御和管理。事实上，终端安全和管理系统在实际上应该是针对网络安全管理人员在网络管理、终端管理过程中所面临的种种问题提供解决方案，实现网络终端的可控管理，并能够支持局域网、广域网构架，达到最佳的管理效果的。要确保网络安全，必须从网络信息系统的整体安全着手，不仅要关注整体信息网络系统的安全，也要重视每台终端的安全。

一、重新认识，改变观念，提升员工意识

安全网关可以阻断由外网向内网发起的病毒和木马攻击，终端安全则可以避免意外感染的病毒和木马在企业内部网中的蔓延扩散。一定要克服终端安全不重要、主机无密可保的麻痹思想，克服网络信息安全是网络管理员和领导的事而与己无关的错误思想，集体重视，团队作战。不仅仅要建立一个强大的网关边界厚盾，更要把每一个终端建成牢不可破的终端城堡。

需要对公司员工进行这方面的培训，指导他们正确使用公司的资源，保护公司的信息安全。进行专门的课程培训，让这些培训在轻松的环境下进行。结合实际情况介绍一些安全常识。比如，向他们介绍在使用即时通信工具的时候应该注意些什么。或者当你在做邮件日志记录的时候则需要按照一定的规范进行，并通过一些现实的例子来告诉他们在紧急情况下应该怎么办，以及为什么要这样做。

二、利用网络管理平台，确保终端安全

充分利用网络管理平台，确保内网用户可信、可控是网络安全的有效基石。比如，应用身份一致性技术，把认证技术与网络环境、政策、行为和安全保持一致，可以检查用户的系统是否被很好地保护，而后决定是否允许接入;及时更新终端的漏洞;控制到每一个 IP、每个 MAC 地址甚至每一个用户，争取让每一个个体都具有保护自我安全、保护全网安全和相互联动的功能;应用安全扫描技术，不定期对用户终端进行扫描，以便及时发现存在的漏洞和弱口令等不安全因素。

结束语：无论是整合还是细分，终端安全管理的发展方向是为用户提供一种可控管的信息安全解决方案，为终端方面的安全问题提供相应的解决手段;提高整个网络中终端用户的实际工作效率;降低终端的故障率，降低网络管理人员和网络安全管理人员的工作量，将网络管理人员和网络安全管理人员从重装系统、杀毒、安装应用软件等等烦杂的低效劳动中解脱出来。在提升终端安全的同时，更不要忽略网关的安全，才能够效提升整体的网络安全。

（作者：石翊　来源：TechTarget 中国）

你是否忽视了终端安全？

企业数据泄漏的事件从未停止过。以今年为例，先有索尼数次被黑导致的用户信息泄漏，再有猖狂的黑客团体 LulzSec 和 Anonymous 接连攻破许多大型网站，如美国联邦调查局，美国中央情报局等，然后 RSA 遭遇了 APT 攻击，其 SecureID 被偷，不得不更换大量令牌。

很多人感叹黑客太厉害，但这只是众多企业遭受攻击的很小部分原因。事实上，大多数企业被黑都是因为自己的安全防护不充分，漏洞和疏忽太多。为什么我们有了越来越多先进的安全技术，但遭受攻击的次数却有增无减？

网络病毒、新型 DoS 攻击、间谍软件、木马、网络钓鱼陷阱及黑客入侵愈演愈烈，企业常常认为堵住、拦住、防住了网络上的攻击就可以实现网络安全了，然而这样是远远不够的。随着各种移动设备的涌入，需要管理的终端设备数量大幅增加。虽然终端资产的数量是最大的，但其重要性级别和关照程度往往会被大幅降低，通常低于网络中承载 ERP、CRM 等与业务直接关联的服务器。如果终端安全受到威胁，即使网络中的核心设备安然无恙，整个网络的业务运行也会受到严重影响甚至瘫痪。

美国安全专家 Mark S. Kadrich 在其《终端安全》一书中曾阐述了自己关于终端安全是影响信息系统安全的根源和通过确保终端安全进而确保网络安全的学术观点。

早在 2009 年来自趋势科技全球防病毒研发暨技术支持中心统计的数据就显示，70%以上的信息泄露和安全威胁都发生在网络终端。

终端安全从提出到现在，在概念上已经经历了很大的变化，从最初是指安装在电脑上的反病毒软件，到后来的包括台式机、笔记本电脑、移动设备的安全防护，再到以网络为中心的访问控制管理，强调所有联网设备的安全，符合企业安全策略所定制的标准，保护网络免受病毒、木马的侵害。

迈克菲公司的最新研究显示，移动恶意软件增长显著且稳定。如何在固有的终端安全保护方案中为各种新的移动设备提供安全，并对各个终端进行统一管理？终端安全管理需要统一的模式。

要建立整体的终端安全防护方案，你可以从以下方面开始考虑：

数量众多的终端设备，规格、配置各不相同，不同终端用户的操作水平也不同。怎样进行有效的管理？或许你可以充分利用网络管理平台。

是否每一个终端用户都知道终端安全的重要性？范围庞大的终端仅靠一支专业的团队去管理和维护是远远不够的。你需要对企业员工进行培训，指导他们正确使用公司的资源，保护公司的信息安全。

终端安全是一个牵一发而动全身的体系，你肯定不希望因为一个终端用户忘记升级、打补丁，致使黑客利用漏洞攻击了公司网络，窃取了数据。那么，你现在就要认真开始制定并执行一套完整的终端安全策略。

（作者：刘平　来源：TechTarget 中国）

你的 Windows 服务器得到适当保护了吗？

你正以何种方式保护你的 Windows 服务器不受恶意软件侵害呢？不管你正在谈论活动目录域控制器、Exchange 或基于 SQL Server 的系统、文件服务器甚至是提供 VPN 访问的系统或者终端服务，你正在做的或许离最好的保护还有些距离。

近两年我才开始看到 Windows 服务器运行各种恶意软件保护。但是为什么恶意软件保护在服务器级别还是没有得到严肃对待呢？可能是因为管理员的这样的想法："它是服务器，没有人真得在上头做太多事情"或者"在与恶意软件的对抗中我可以不会信任我的用户，但是我很自信我不会在服务器上有任何错误步骤会导致一次恶意软件感染。"在这一事件上每个人都有自己的想法。

如果你不想被攻击，你应该更加超前地保护你的 Windows 服务器。我最近工作的一个项目没有发生且一个企业终结了上千个系统，包括全世界范围内的几十个半路被高级持续性威胁（APT）感染的 Windows 服务器。有些服务器受保护了有些则没有。正是这些不一致性会对你不利。不仅如此，你的业务可能受到一些遵从规则的约束，如 PCI DSS、HIPAA 和其它。或者也许你的法律团队已经同意了包括恶意软件保护在内的契约或服务等级协议（SLA）。

不管你打算或实际怎么运用你的 Windows 服务器，它们都很有可能处于恶意软件感染的危险中，理解这一点很重要。这不只是你高度可视的生产系统，而是全部。和谈到执行信息安全评估时我给客户的建议一样：任何事情都是公平的，你为什么只看到环境的小部分呢？坏人和恶意软件不了解界线，所以你保护好跨越企业的所有事情会有更好效果，包括那些你认为战略上看不重要的 Windows 服务器。

以下是你可以自问来帮助更好处理 Windows 服务器保护的 10 个问题：

1. 我们准备应对哪些流氓软件威胁？我们是否在事故响应计划中记录了这些威胁？
2. 我们应该对什么规则、策略和合约负责？
3. 我们是否需要执行实时扫描？
4. 是否有些文件/文件夹排除需要合并到杀毒软件配置来杜绝其它问题的瓶颈？
5. 我们是否需要 Web 浏览器级别的额外保护来阻碍钓鱼（phishing）和浏览器相关的攻击？

6. 管理员是否在我们的服务器上检查邮件？有更好的方式来帮助最小化这些风险吗？

7. 全系统扫描的最好方法是什么？需要进行全系统扫描吗？

8. 我们是否只需保护 OS 卷或者我们的数据卷是否有可能感染的文件？

9. 除了生产服务器之外，还有其它什么物理或虚拟的 Windows 服务器需要保护？

10. 我们的边界或是基于云的杀毒软件是否提供足够的保护来判定没有运行任何服务器级别的东西？

回答完这些问题后，你应该审查微软运行在 Windows 服务器上的一套用于杀毒软件的基本指南。审查是有收获的。

如果你真得深入并思考这些问题，你可能会发现你的服务器处于应对恶意软件的保护中。如果你选择在你的 Winows 服务器上发装杀毒软件，把注意力放在正确的目标上。你不用担心哪个杀毒厂商是最好的（我不认为有最好的解决方案），只需关注保护你的服务器不受恶意软件侵害的最佳方法。这意味着你可以在你的 Windows 桌面上运行相同和不同的杀毒软件。

只有你自己知道什么是最好的。赶快行动吧！

（作者：Kevin Beaver　译者：Mark　来源：TechTarget 中国）

Windows 服务器补丁你伤不起！

想像下这个场景：你运行着 Exchange、SQL Server、Active Directory 和其它类似产品的关键 Windows 服务器完全暴露在运行 Metasploit 的内部人员面前，而恶意软件为外来攻击者提供了远程访问。

你大叫道："不，这不可能在我的环境中发生，因为我一直都有给 Windows 服务器打补丁。"可是，事情没有这么绝对。

除了运行在工作站的固态完全磁盘加密和智能手机上的零控制外，Windows 服务器上的缺少的补丁也是可预测的漏洞。由于某种原因，从 Server 2008 R2 一直往回到 Windows NT 的基于 Windows 的服务器都没有恰当地得到修补。追溯到 2001 年，在我的内部网络漏洞测试中，Windows 补丁（不是服务包）可能在任意给定数的服务器中漏掉。这不只是 Windows 服务器中的问题。工作站几乎总是在更新。

首先，我会怀疑问题很常见，"我们不能修补服务器，因为如果我们这么做了，厂商可能就不支持该应用了。"但是我进一步深入就发现，通过 Windows Server Update Services（WSUS）和其它第三方系统，这些 Windows 服务器都在修补范围内。也许偶然漏掉的补丁与网络管理员卸载某些补丁来解决问题有关？也许补丁管理过程中有些事情出错了，比如责任方的疏忽？

因为某些原因，WSUS 和第三方补丁管理工具都不会报告这些遗漏补丁。似乎是补丁越老，它被忽视和暴光的机会越大。你会希望在这里或那里找到一个遗漏补丁，但这在很多项目中是一个持续性问题。

不管潜在的起因是什么，你网络中现在在 Windows 服务器上遗漏补丁数量的比率很大，明白这一点很重要，这些补丁都在等着流氓软件和内部盗窃的利用。

解决方法是什么？最好的做法是返回并确保所有的 Windows 服务器补丁都显示安装了。接着，信任但要查证。你可以通过运行任意数的漏洞扫描器来完成，如运行 Qualys、Guard、NeXpose、Retina 或 LanGuard 来确定忽视了什么。即使你只是使用扫描器的试用版或免费版，你将有可能看到我所谈到的东西。

你无须认证就可以运行这个漏洞扫描器，也许从进入你网络的人的角度，但并不通过 Windows 域或任何特定 Windows 主机的认证。如果扫描器足够好，它只会找到你需要的东西。

最近，我在这方面更进一步，我用常规的域用户凭证运行认证的扫描。这类扫描会找到相同或者可能更多的遗漏补丁并提供在你网络中可以看到和利用事物的更精准代表。

关键的事情是要明白你可能得不到 Windows 服务器的精确补丁信息。不好的信息等于不必要的风险。假设每件事情都很好，这可能产生安全上严重的错误感觉，尤其是考虑到内部人员运用 Metasploit 攻击你有多容易时。如果你没有执行周期性的内部漏洞扫描，那么现在就是开始的绝佳时机。

（作者：Kevin Beaver　译者：徐艳　来源：TechTarget 中国）

Linux 服务器系统最佳安全实践

维护一个企业级的安全的计算环境需要设计策略和过程从而使得对系统和数据的未授权访问降至最低。为了保护基于 Linux 的计算机资产免于这些威胁，像许多其它以安全为核心的过程一样，你必须知道你想保护什么以及别人可能会如何尝试获取访问。成功的安全管理是心态。也就是说，像坏孩子那样思考。

在本文中，我们将会讨论基于 Linux 的服务器系统的风险评估。

确保你的 Linux 服务器系统安全的第一步是正确地评估所面临的风险。只有这之后企业才能部署一套有效的防护措施来预防、侦测，并且如果需要的话对于可能发生的违规正确地做出反应。

首先，辨识需要保护的 Linux 资产。资产可能包括硬件、软件、数据或像 email 或 Web 站点主机这样运转的服务。每个资产都具有价值，要么是货币价值要么是未来可能带来收入。

接着，辨识每个资产面临的潜在威胁。威胁可能来自组织的内部或外部。一些内部威胁只不过是偶然的，但是有些可能是恶意的。

对于资产的威胁依赖于攻击的动机和攻击者如何获得对资产的访问。动机可能是纯粹的挑战，伤害资产的拥有者，或是为了谋利。攻击者可能想访问你的数据或只是拒绝合法用户的访问。每个威胁都有被利用的必然的可能性，这通常与资产的价值相关。虽然在组织内广泛地了解和变化会有困难，但是使用一个风险管理框架来给每个辨识的威胁分配一个可能性，会帮助你对缓和这些风险需要采取的行动进行优先级安排。

尽管不可能列出所有潜在的威胁途径，但一份最常见风险的概述能让你开始自己的风险评估。

最棘手的威胁途径是用户。尽管有各种的保护机制，人们仍然会被愚弄或被要挟做出不恰当的行为。用户的意识、培训和访问权限是缓和任何 Linux 风险的重要部分。

密码在任何计算环境中经常代表着最常见的软肋。为了辨识不安全的登录密码，运行如 John the Ripper 这样的密码有效性检查器。应用和数据库的密码也应该检查“可被破解性”或是进行修改以便满足这样的需求。同时，辨识 Linux 服务器上不需要的访问授权。例如，如果密码文件（/etc/passwd）被远程地分发（通过 rcp/rcopy 程序或 NIS 服务），用户可能会对从未使用的服务器具有登录访问权限，从而创造了毫无好处的潜在的威胁途径。

另外一个主要的威胁途径是网络。任何能访问你的本地网络（物理的或是无线方式）的用户有可能试图连接到网络上任何其它的资产。所有的 Linux 系统运行开放的网络端口，并等待来自网络查询的程序。每个这种服务都代表者一个威胁途径，要么通过欺诈的认证，或是由于软件瑕疵可能错误地允许访问。使用 netstat 命令来找到系统所有的开放端口。

使用 Nmap 工具扫描网络上其它机器的开放端口。每个开放端口代表着一个威胁途径，应该被关闭或是监控非法的访问。不要忽视任何传统的拨号访问点。防火墙是可信网络和不可信网络（如因特网）之间的边界。你的防火墙应该配置只在已知和需要的端口上传输数据。防火墙传输数据的每个端口同样都是一个威胁途径。

除了正常的监控以外，你还应该同时检查日志来关联需要的访问。Lastlog 命令显示用户的登录信息。可以在路径/var/log/messages 下发现各种各样的日志信息。许多应用和数据库也提供记录机制来追溯用户的访问。检查这些日志，你可以观察当前谁在使用和（可能）需要访问特定的资源。

无论什么复杂的软件都是有缺陷的，但是只有当缺陷以不受欢迎的行为表现它们时才会被了解。通常的 bug 只会破坏数据或是引起宕机，但是有一些会造成无法预料的后果，比如允许未授权的访问。这明显地表示为主要的危害。攻击者不断地搜索着这些类型的 bug，而厂商们则在发现这些 bug 时，尽力快速地修补它们和提供软件补丁。你所能做的是确保定期地检查和更新你的操作系统和应用软件。

检查 Linux 服务器上软件更新的过程依赖于应用或是 Linux 版本。例如 Ubuntu 版本的 Linux 提供一个更新管理器（通过菜单“系统>管理>软件源”可以发现），可以配置每天进行检查更新。你越经常性地检查更新，你的漏洞窗口越小。同样对于来自未校验来源或作者的免费程序或软件要小心谨慎。

需要监控和保持更新的最重要的软件是面临外部环境的软件，如 Web 服务器和网络应用（如 VPN 或 SSH）。Web 服务器软件定期地检测糟糕的配置和 bug。Web 应用可能会遇到恶作剧的输入数据来进行不正当的应用。大多数的 Web 应用语言，像 Perl、Python、Ruby 或 PHP 有工具或可用的附件来净化输入数据以及禁止用户输入的代码，如 SQL 或 Java 脚本。你的 Web 服务器或是其它面临外部环境的应用接收来自用户的数据都意味着可能的威胁。同样，检查这些程序产生的任何日志文件有助于你辨识合法和非法的访问。

（作者：King Ables　译者：Odyssey　来源：TechTarget 中国）

移动设备网络防御战略

不负责移动设备的管理者可以通过维护关键设备，如公司邮件服务器、移动应用网关、远程登录集中器和网络门户，来使得他们的网络可以抵御移动恶意软件。

例如，大多数企业已经在电子邮件出现在终端用户前进行了过滤，从而屏蔽掉垃圾邮件和钓鱼网站。无论反垃圾邮件措施是在企业邮件服务器还是在托管的电子邮件提供商处实施的，都会使移动设备受益。但是，一个必要的措施可能是设法确保所有的移动电子邮件都通过这些过滤器传递，可行的方法是阻止企业电子邮件发送到个人的 POP 邮箱中。

当移动设备通过应用网关或远程访问集线器（remote access concentrator）访问企业网络时，恶意程序可能被设备指纹或内容监测工具阻止。例如，设法限制通过设备标示符或支持的操作系统/浏览器类型对设备的访问。通过网络反病毒、入侵防御系统(IPS)或统一威胁管理（UTM）平台，转发所有通道上的流量，丢弃可疑的信息。但这些措施并非固若金汤，现有的网络防病毒系统或许能检测出 Win32 蠕虫病毒，但对这些病毒的 Windows Mobile 版本不一定同样有效。但是，它们可以帮助将网络与安全威胁隔离开来，因为这些威胁可以使用不受保护的移动设备绕过台式机或笔记本的防御体系。

一个万无一失的、能够阻止企业数据被移动恶意软件窃取的方式是：阻止敏感数据存储在移动设备上。可以考虑让移动应用程序和数据访问使用只读端口。例如，在图像（而不是文本）格式下呈现应用的内容，阻止文件和附件下载。你需要决定哪些类型的内容应该还是不应该放置到移动设备上，权衡移动设备的使用和商业风险的关系。

PDA 和智能手机安全的未来

从长远来看，多数管理者将把移动终端和基于网络的防御措施结合起来，像对待笔记本电脑和平板电脑那样对待智能手机和掌上电脑。然而，高速无线广域网连接的出现有可能会提供更多的移动安全防御措施。

例如，一些运营商已经可以为所有的移动设备提供与操作系统无关的、电子邮件和手机短信过滤服务。相较于为智能手机和笔记本安装常驻系统的反恶意软件程序，“云端”战略或许可以提供更为简单的方法。展望未来，企业应设法使用安全的无线广域网服务，从而减少各种来自恶意软件的威胁。

（作者：Lisa Phifer　译者：Sean　来源：TechTarget 中国）

针对企业 iPad 终端整合的安全策略

随着人们不断地提高笔记本电脑的安全性和集成度，笔记本电脑的功能已经足够强大。那么，如今涌入产业界的下一代网络终端设备的性能又如何呢？平板电脑现在在业界正炙手可热，其中的佼佼者便是苹果的 iPad。毫无疑问，在接下来的几个月里，iPad 在企业中的应用将会增加。

要高效地使用这款流行的平板电脑，工人需要访问企业的应用程序和数据，但这也意味着企业的程序和数据等资源不能违反相关政策，并且不能对 iPad 进行“越狱”。接下来让我们讨论讨论，对于那些想要将 iPad 作为其企业网络终端的人们来说，集成 iPad 都有哪些方法。

方法 1：来宾终端（Guest endpoints）

作为一款支持 Wi-Fi 的设备，iPad 能够接入任何开放的无线局域网（WLAN），包括来宾式无线局域网(guest WLANs)。因此，一种在网络中集成 iPad 的方式就是默认将员工拥有的 iPad 当做来宾终端，就像对待其他无法管理的来宾终端一样。

网络访问控制（NAC）产品通常用于控制来宾对网络的访问，如对来宾接入网络的时间进行限制，或者在接入前对其进行安全扫描。但是，NAC 服务器无法持续地为 iPad 布置 NAC 客户端，也不能强制 iPad 运行基于浏览器的安全扫描。因此，我们只应给予 iPad 基于 Web 或因特网方式的接入权限。

在这种方法中，网络访问控制器和网络入侵监测系统可配合使用，用于识别 iPad、监测终端接入系统后的活动以及断开“不守规矩”的设备。虽然这两种技术能够提供可视化功能，并且也能够保护网络，但是仅对 iPad 设备提供普通的来宾访问权限并不能使其成为一个（真正意义上的）企业用网络终端，相反还会限制该设备的能力。

方法 2：远程终端（Remote endpoints）

另外一种方法是将 iPad 当做远程终端来使用，即便是在本地无线局域网内也可以这样做。例如，已接入英特网的 iPad 可以通过 Exchange ActiveSync（交流同步）检索公司邮件，或者使用由思科系统公司或 Juniper 网络公司提供的 VPN 客户端来获得比来宾账户更大的网络接入权限。

我们可以要求 iPad 的使用者浏览预提供的网络地址，安装配置档案进行批量系统设置，这些设置包括设备的加密和密码要求、数字证书、VPN 和 Exchange 的使用参数及使用限制

（如禁用摄像头）。配置档案能够被锁定并加密，以防止共享或者篡改，但关键还是在于强制执行配置档案；安装配置档案也不能够确保每一台 iPad 都兼容。

要解决这个问题，一个办法是每当电子邮件被阅读时，使用 Exchange ActiveSync 检测被选择的 iPad 的配置情况，剔除不兼容的终端。例如，在 Exchange ActiveSync 的政策设置里我们可以阻止未签名的应用程序阅读公司邮件。同样地，它也能够将政策设置传递给那些拥有 Exchange 访问权限的 iPad，iPad 还可以被设置为定期刷新这些政策设置。

另一种办法是安装与 iOS 兼容并具有整体系统评估能力的 VPN 客户端。例如，Juniper 公司的 Junos Pulse Mobile Security Suite，该套件结合了 SSL VPN 技术与终端安全措施，如反病毒、反垃圾邮件以及接入企业网络所必需的应用程序控制等。该 VPN 客户端甚至可以在受理相同的身份认证、整体监测或授权策略时自由地在 Wi-Fi 网络和移动通信网络之间漫游。我们还可以选择使用思科的与 iOS 兼容的 AnyConnect。

方法 3：受控终端（Managed endpoints）

最后，我们来讨论控制式的终端。许多企业通过采取某些移动设备管理（MDM）控制措施来实现对 iPad 的完整集成。这可以在如今运行 iOS4 的 iPad 上面实现。

在 iOS4 中，苹果为供应商如 AirWatch、BoxTone、MobileIron、Sybase、Tangoe、Zenprise 等提供了远程访问接口。通过这种方法，使用者通过浏览预提供的网络地址在公司的 MDM 服务器和 iPad 之间建立连接。然后，MDM 的请求和响应由苹果的推进通知服务（Push Notification Service）转发。通过这种渠道，配置档案和企业应用程序将通过无线网络被发送至受控制的 iPad，同时终端配置和应用事件也可以发送回 MDM 服务器。

这些技术能够为系统提供近乎实时的完整评估和执行能力。例如，配置档案可被用于配置企业的 VPM 或者 Exchange 访问权限。如果访问权限之后被吊销，MDM 可以移除配置档案，删除所有相关的企业数据，包括电子邮件信息、联系人和日历条目。同样地，如果 MDM 检测到某一 iPad 被“越狱”了，那么该 iPad 与 MDM 服务器之间的协作关系可被解除，之前 iPad 上所安装的企业应用程序也可以被禁用。

苹果限制了 iOS4 MDM 能控制的配置以及可执行的命令。具体而言，你不能强制安装受推荐的苹果商店应用，这会使得你可以很方便地安装安全程序如 VPN 客户端或恶意软件扫描程序。虽然 iOS4 的版本可以被检测到，但目前还无法通过无线网络进行 iOS4 的更新；更新仍然必须通过 iTunes 进行。

然而，MDM 产品目前已经开始使用这些接口在 iPad 上评估和执行某些特定规范。例如，AirWatch 能够根据预先提供的黑名单，检查安装在任何 iPad 商店应用程序，从而采取相应的措施，如警告用户或者远程卸载 iPad 上的违规程序。MobileIron 可以（当然它的功能不止于此）在任何拥有过期的管理策略、被禁用的加密、未授权硬件版本等的 iPad 上删除 Exchange、VPN 或者 WLAN 配置档案。

总结

像 iPad 这样的平板电脑需要新的工具去实现、评估和执行终端集成。但是，同笔记本电脑和上网本一样，iPad 的安全策略控制方法繁多，有高度可视化/触摸类的工具，也有可提供广泛控制的高度集成工具。有些企业可能会根据需要同时采取多种方法，例如，控制管理那些装有企业程序的 iPad，同时将那些没有安装企业程序的当做普通来宾。要学习更多有关 iPad 配置档案和安全设置的内容，请查阅苹果的“iPhone in Business”（PDF 文件）指南。

（作者：Lisa Phifer　译者：Sean　来源：TechTarget 中国）

移动设备：企业安全策略

在2007年Gartner公司无线与移动高层首脑会议上，分析师们描绘了一副可怕的场景来表述各公司陷入解决移动和无线安全问题的困境。按照John Girard的意思，超过三分之二的企业会经历由于移动用户不恰当地连接到不安全的服务或者下载恶意应用程序引起的安全问题。分析师John Pescatore预测说，在2007年移动恶意软件会变得司空见惯，在2009年上半年攻击会引起真正的业务中断。幸运的是，大部分这些恶意攻击利用的漏洞是可以确认并解决的。在本文中，我们会盘点一些使移动设备无线服务安全的策略。

网络犯罪：正在通过移动设备靠近你

无线PDA和智能手机已经使用了很多年，但很少有关于安全鞋漏的头条新闻爆出。Pescatore提出：不安全的移动设备已经飞到了雷达下面，因为移动设备恶意软件编写者受到了平台和操作系统多样化的限制。他说：“肯定已经存在了一些移动恶意软件，但是这些软件大部分没起作用，造成的实际破坏很小，而且也没有蔓延开来。”例如，最近McAfee调查了200个移动设备用户，发现83%的用户遇到过移动恶意程序的攻击，但是这些事件中只有五个影响超过了10万台移动设备。

然而，恶意软件的影响可能会发生变化，随着移动从业人员的增多，移动环境变得越来越统一，业务系统的连接面更广了。“现在已经到了企业开始部署安全进程、架构和控制来防御移动恶意软件的年头了”，Pescatore建议说，“大量蠕虫和病毒不是真正的威胁……移动恶意软件会更有针对性地对特定的设备，应用和业务出现。企业保护策略需要寻求新思路开发新方法”。

移动服务使用的无线接口是另一个病毒传递攻击的方向。John Girard相信存在范围很广的无线服务攻击很少，因为运营商会保证他们自己的网络安全。他说：“数字卫星和电台网络采用双向认证和强加密方式，阻碍试图窃听，跟踪通信或者解密数据和声音流的行为”。形成鲜明对比的是，Wi-Fi和蓝牙攻击频繁，这是由于遗留的漏洞未打补丁，也由于终端用户的配置不当。“智能手机Wi-Fi功能仍然不幸地是重复（那些相同的】老问题的另一个漏洞。”

逆转形势

大部分公司都很熟悉Win32恶意程序和无线漏洞。保护商业PDA和智能手机的一个有效策略是需要结合已有的最佳实践和新技术新工具。

1. 像 Win32 记事本程序一样，具备 Wi-Fi 和蓝牙接口的移动设备必须安全地配置好，利用健全的数据链路安全选项（如 WPA2-Enterprise），禁用有风险的选项（比如发现蓝牙设备）。内部无线网络中的活动可以通过最佳实践（如 802.1.X 和 WIPS）来监视和控制，它不依赖于客户端设备的类型。在从 3G 运营商漫游到公司无线局域网，到公共无线热点区域时，为了实现统一的端到端通信安全，将会需要像移动 VPN 这类新工具。在 3G 服务可用，而且比较廉价的地方，移动设备可能会为了降低风险考虑，把那里提升为热点区域（hotspot）。最终，公司应该设法给所有新移动商业应用和客户端服务器接口加上安全措施。

2. 移动设备可以配备客户端安全措施，类似于一直在 Win32 记事本上使用的安全措施，从加电验证，数据加密和备份恢复到防火墙、VPN 以及防病毒。移动操作系统目前仍然处于追赶竞争对手的发展过程中，所以经常需要额外增加专门为移动设备上运行设计安全软件。Girard 估计到 2010 年的时候，每年在所有这些移动安全工具上的花费将会超过一开始购买一台普通智能手机的成本。各公司可能想给在关键业务流程中使用的 PDA 在这方面做短期投资，所以就强烈要求在将来向供应商购买的移动设备中带上这些安全功能。然而，Pescatore 警告不要单单依赖于客户端移动设备杀毒。他说：“在绝大部分同类的 Windows 平台上，这都是不够的， 将来在同类移动设备上也是不够的。”

3. 相反，移动客户端安全措施应该辅之以服务端保护，包括在公司邮件服务器和移动通信服务器上的恶意软件清除。“企业应该关注同步服务器，无线应用网关和从 2007 年开始提供服务的外部无线网络服务提供商，关注在这些方面恶意软件内容保护的投资，”Pescatore 表示。企业还可以在服务端采取措施，比如：文件活动监视，数据库活动监视，用消息内容过滤来跟踪和控制移动设备对公司数据的使用。最后，网络网关可以使用网络访问控制（NAC）授权有选择的访问给属于员工的移动设备，或者阻止私自接入公司的移动设备访问。这些多样化的措施可以有效缓解大范围的问题，但是他们都需要在 IT 部门控制之下（至少在一定程度上）才起作用而且对移动设备用户是透明的。为减轻 IT 机构负担，一些公司可能采取从无线运营商或者第三方机构（比如 iPass）外购一些移动安全方面的任务。

结论

现如今大部分商业用途的 PDA 和智能手机都是“自带便携”型的设备。许多雇主都没办法列举出所有访问他们网络、服务器和数据的设备，能快速采取行动阻止主流移动设备恶意软件爆发的就更少了。第一次爆发可能很快就会出现，也可能几年也不出现。不管是哪一种情况，

开始考虑移动设备安全策略已经成为了一种简单的常识。你可以通过对你单位全体员工已经在用的移动设备建立清单来估计问题的大小，按照商业风险采取短期行动减轻当前移动环境中的脆弱性。然后在没有把安全策略纳入长期计划前，抵制住部署移动应用和设备的诱惑。

(作者：Lisa Phifer　译者：Eric　来源：TechTarget 中国)

保证移动办公用户的安全

在跟上员工的移动办公步伐上，Kenneth Johnston 并不是一个人在战斗，Johnston 是担保银行（guaranty bank）信息系统的副总裁兼 CIO。对员工而言，扩展银行现有电子邮件在移动设备上的加密功能，是一个痛苦和耗时的过程。

Johnston 说：“我们的移动办公人员和客户设法避开身份验证过程，但失败了。实际上，加密电子邮件非但没有增加安全保护，反而加深了我们对数据泄漏的恐惧。”

于是 Johnston 转向 Proofpoint 移动加密技术，以帮助银行员工和他的银行商业客户扩展电子邮件加密功能。Proofpoint 允许用户以一个移动应用程序或者 Web 访问的形式使用其电子邮件加密服务。

位于美国密苏里州斯 Springfield 的担保银行部署了一个有效的 Proofpoint 企业套件，用以防止非认证的电子邮件收发访问。Johnston 说，移动应用程序是一个企业套件的自然延伸，为用户提供了一个熟悉的使用体验。现在，员工和客户可以快速验证，并直接在他们的设备上打开消息。

由于移动办公越来越普遍，安全厂商适时采用了新的移动设备加密安全手段，如智能手机加密。在三月份，Proofpoint 推出了新的移动应用，使移动用户可以轻松对加密信息进行解密，并支持在电子邮件文档中进行搜索。对安全厂商来说，使 IT 移动管理更容易是一种日益增长的趋势。

Ogren 集团的创始人兼首席分析师 Eric Ogren 表示，在移动设备上的扩展认证和加密已逐渐成熟。早在 20 世纪 90 年代，RSA 就在 Palm Treo 上支持 SecurID。其他新近加入的厂商包括 Overland Park,堪萨斯州的 PhoneFactor，它们提供了基于手机的无令牌双重认证系统。Ogren 表示，对不断增加移动办公设备的公司而言，延伸到智能手机和平板电脑上的安全产品是一个更有吸引力的选择。

Ogren 说：“公司最大问题之一就是在移动设备、笔记本电脑、台式机等所有设备上取得认证。将密钥嵌入到设备以便最终用户可以查看加密电子邮件是非常有效的。”

其它安全厂商也加入了战斗。旧金山的移动安全厂商 Lookout 销售在 Android，黑莓和 Windows Mobile 设备上的移动应用软件，它可以检测移动恶意软件并分析应用程序是否在执行一个隐蔽的入侵。和其他的移动设备平台一样，Lookout 执行安全备份，这可以定位失踪的

设备和执行远端清除功能。包括赛门铁克，McAfee 和趋势科技这些主要的安全厂商也提供类似的功能。

总部位于洛杉矶的 Wedbush 安全公司的副总裁和 IT 主管 Mattias Tornyi 表示，他的公司专注于针对周边设备的攻击已经很久了。但他承认，周边设备的定义不再是泾渭分明的，SSL VPN 功能是必备的。虽然使用 BlackBerry 的服务可以使公司安全地进行管理，许多经纪公司的在外场办公的员工都在使用 BlackBerry 设备，但越来越多的人转向了苹果 iPhone 和 Android 设备。我们的目标是能够安全地将帐户信息迁移到 iPad 和 iPhone 上。

Tornyi 说：“我们现在只处理随时，随地地访问这个概念。我们在保护所有的一次性令牌，我们也有正在使用的高性能的防火墙和‘入侵防御系统’。这将是一个缓慢的过程。”

(作者：Robert Westervelt 译者：Sean 来源：TechTarget 中国)

建立安全策略应对移动设备威胁

在过去的十年中，我们的工作场所发生了很多变化，其中最大变化之一就是企业的大量信息可以离开办公室，并在雇员的笔记本电脑和智能电话中不断地移动。十年前，雇员很少在家中或是在路上工作，当然不会背着笔记本电脑到处跑。随着企业移动设备的激增，伴随而来的是信息遭受外部窃取和恶意访问。

更糟的是，攻击者都理解存储在移动设备中的企业信息的价值，并开始采取针对性的手段。

由于企业信息的价值要远远超过设备自身的价值，所以专家们建议，IT 管理者要有一套移动设备的管理计划，要能够在设备被盗时恢复信息。

在企业准许用户将其移动设备连接到网络，并下载机密的企业数据时，不管这种数据是内部信息或是客户的数据，我们都需要一套安全策略，最起码要规定设备应当如何加密。

建立策略

企业需要为移动设备的安全进行预算，因为在发生硬件丢失时，IT 部门需要认证工具及类似的专业软件来跟踪设备并删除其中的数据。

IT 管理者应当重视设备内部和外部的认证。许多可用的企业级移动设备平台包括了比普通设备自身内部所安装的认证更为强健的认证。相同的认证策略可用于所有不同类型的设备，并可推广到整个网络。

这种认证意味着在雇员每次访问设备时都必须输入口令。IT 管理者必须确保口令难以猜测，并且雇员不会将口令粘贴在某个明显的位置（如笔记本的电脑包上等）。

也许要求雇员在每次检查新邮件时都需要输入口令有点儿麻烦，但是这样做可以提醒雇员：你正在使用包含着机密信息的设备进行工作。

当然，企业的移动设备安全策略需要最适用的规则，要提供充分的帮助信息。IT 管理者要警告雇员不能将移动设备随意放置在饭店或酒吧的桌子上，而应当随身携带。在旅馆住宿时，如果不使用设备，要将其锁在保险箱或其它安全设备中。

要警告雇员，无论是工作用的笔记本电脑还是智能手机，都不要轻易允许他人使用。

设备被盗怎么办？

企业的移动设备安全策略还应当概述雇员丢失设备后应当采取的措施。通常，这种措施意味着与响应中心联系，或与 IT 部门或公司中的负责人联系，以便于及时关闭设备。

移动设备的安全策略还应当要求 IT 部门在笔记本电脑上安装设备保护机制，要安装能够远程擦除失窃设备数据的软件。谨记，移动设备的跟踪软件依赖于主要芯片厂商生产的芯片中所嵌入的技术。

在笔记本电脑丢失或被盗后，在该设备连接到互联网时，跟踪软件应当与包含 GPS 功能的设备芯片保持同步，从而可以跟踪并定位设备。跟踪软件还可以远程擦除所有的机密企业信息。此外，这种跟踪功能也可用于智能电话。

安全策略未必过分苛刻。通常，这种策略只需规定一些可行的关于设备使用的常识，并与特定的硬件和软件相结合，在 IT 部门的帮助下保护企业的敏感信息。

（作者：茫然　来源：TechTarget 中国）

制定网络终端安全政策　防御恶意攻击

企业安全所涉及的范围正在迅速减少。从公司的财务信息、源代码邮件、非结构化文件到其他形式的数据都游离于企业防火墙之外，在非 IT 控制设备上。剑桥和 Forrester 研究公司发现北美和欧洲的企业里有一半左右（47%）企业认为为第三方合作伙伴执行安全需求是很重要的。

IT 界的安全长期以来都遵循一个简单的原则：公司拥有所有用户的终端设备（访问公司信息），设备安全了其上的数据也就安全了。但是如果这个原则不再适用，那会怎么样呢？敏感信息在非公司所属设备的储存和传输的不便越来越明显，表明这个原则是行不通的。

从事制造、媒体和季节性服务的企业之间的对话揭示了一个非常规的但却充满智慧的概念：控制并不一定需要所有权。不仅这样，要成功地控制敏感信息在网络上的传播就需要彻底扭转传统的概念，即假设企业没有任何设备的控制权。Forrester 研究公司把这个策略称为零信托模型。对这个策略更为简单的解释就是：假设所有终端设备都是不友好的。

在最近的研究中，Forrester 研究公司列出实行零信任策略的五个数据安全设计模式：瘦客户机、瘦设备、进程保护、数据保护和跟踪。所有的这些模式都假设企业没有终端设备的拥有权。将所有权和控制权分开，企业能够设计出一个网络终端安全政策，它包含了所有可能的所有权形式，如“技术大众主义”、境外生产和外包。最终用户可以通过以下方式来保障公司的信息安全。

1、瘦客户端：进程集中化，信息本土化

瘦客户端很早就被零信托计划策略采用，它集中了很多技术。像流媒体服务器、虚拟主机桌面技术和虚拟工作间技术。为了加强它的安全性，须将敏感数据集中在安全性能更好的设备里，远程设备只有通过瘦客户机的终端应用程序才能进行数据访问。由于这里需要与网络对接，所以瘦客户端不支持脱机使用。

瘦客户端的优点是数据从不离开服务器：它只将数据提供给终端设备。出于安全考虑，IT 能够限制主机的粘贴复制操作，限制数据转移，并要求使用 tokens.Client 进行两方身份验证。

2、瘦设备：出于设备安全考虑，使用备份数据

瘦形设备模式通过限制允许访问数据的设备类型来控制访问途径。智能手机等设备只能储存一定量的敏感信息。它们所储存的信息是复制而来的，原始数据则储存在数据中心。由于它们的体积、储存容量和处理速度的限制，应用程序被局限在电子邮件、小规模浏览网页和简单的网页程序中，根本谈不上通常的数据处理。而在薄形设备模式中，IT 安全团队仍能控制设备的安全，即使他们并不具备设备的拥有权。使用本土的管理工具或者第三方移动设备平台，如 Sybase 公司的产品，可以通过备份和强制加密等加强智能手机的安全。出于安全考虑，瘦形设备可以被远程移除，做到真正意义上的可控制，这点与 PC 机不同。然而，在不属于自己的设备上强加 IT 安全政策会存在技术上或者政策上的不便。

3、进程保护：在一个安全的环境中处理本地信息

瘦客户机模式中用户设备不储存敏感信息，但进程保护模式与此不同，它允许数据运行在非 IT 所有的设备中。一个独立进程环境中的敏感信息，即从用户的本地操作系统环境中分离出来——基本上是一个“气泡”——其中的安全和备份性能是由 IT 控制。进程保护模式有很多优势：本地执行、脱机操作、中央管理和一个高精度的安全控制，包括远程擦除功能。但是要记住，大多数操作系统和应用虚拟化产品仅支持英特尔或 Windows。

4、数据保护：文档自我保护不受位置限制

鉴于以前的模式都设法通过控制运行环境来处理信息，而数据保护模式保护的是数据本身。如企业版权管理（ERM）这样的技术可直接访问文件规则。无论文件放置在何处，这些依靠密码方式强制执行的规则都是适用的，这是一个重要的优势。所有零信托数据安全战略里的模式保护数据都是最精细、最有效的，因为它的重点是信息，而不是信息的载体。

这种模式缺点之一是，ERM 的每个终端都需要客户端代理。该技术还会给部署带来挑战：一些机构告诉弗里斯特研究公司，ERM 的商业客户制定的政策有时过于严厉，使得数据难以获取，而且政策不能很好地适应机构改革。

5、跟踪：明确重要的信息移除的时间

零信托数据安全设计的第五种模式使用的是补充数据检测控制技术，用来检测、记录和选择性封杀物理或逻辑企业边界的敏感数据。数据泄漏防护（DLP）技术和较小程度的安全信息和事件管理（SIEM）工具，是这一模式的重要组成部分。

该模式的主要优点是，它可以检测敏感数据，因为它在逻辑安全边界以外运行，所以它能很好地理解信息流的速度和方向，并发现异常传输。不幸的是，大多数企业都不能要求其业务

伙伴在他们的计算机上安装的 DLP 代理。基于这个原因，企业应把空中监管模式作为个人电脑保护的一种补充。

（作者：Andrew Jaquith 译者：Sean 来源：TechTarget 中国）

终端数据丢失防护部署中的五大安全技巧

部署终端数据丢失防护可能是所有 DLP(数据丢失防护)项目中最令人恐惧的一步。软件供应商提供的功能集五花八门，恐怕没有哪个组织可以毫无忧虑地加以处理。

这里有五个技巧可以帮你避免常见的隐患，同时成功的保护企业数据：

1. 在静态工作站镜像上测试是非常不错的，但数据丢失防护的大多数问题出现在首次将其部署到使用数据的用户。在你推出部署数据丢失防护解决方案的第一个部门确定一些关键用户，根据需要对他们进行培训，并在测试阶段与他们密切合作。通过关键用户的帮助，可以避免非技术业务部门测试中出现的问题，也可避免部署中没有任何用户反馈的情形发生。

2. 确保你的目录服务器是最新和准确的（这实际适用于任何形式的数据丢失防护部署）。如果你试图根据计算机组而不是用户角色来管理策略，可能会产生策略冲突（特别是当用户发生了变动）。大部分组织将他们的数据丢失防护策略设计成根据用户角色应用不同的策略，例如，财务部门就比客户支持代表有更多的自由来处理财务信息。即使一个计算机组已经映射到一个业务单元或该业务单元中的一个特定用户，在下次更新时可能会破坏该策略。依据用户以及组或者角色要比依据计算机来管理好得多，即使这意味着你首先需要花一些时间对你的目录服务器进行调整。

3. 建立适应用户在你的数据丢失防护网络内和非受控的网络之间变化的策略。例如，在你的网络内有一个数据丢失防护策略检测和阻止你的客户数据库中的信用卡号传输，当终端离开公司网络时，在终端上的策略发生变化，允许正常的使用信用卡。这是完整的数据丢失防护工具和其终端代理诸多特性中的一个，但不是全部。部分文档匹配和数据库指纹策略非常占用内存，远远超过了用户的笔记本和台式机的能力（假如用户在数据丢失防护之外还要处理其他的事务）。切换一个模式匹配策略，例如正则表达将会增加误报，但会减少对电脑性能的影响。你也可以设置策略切换到监控/警告模式，而不是阻塞模式来进一步减少对用户的影响，虽然安全风险较高。

4. 首先关注终端发现和 USB 保护。在一系列的终端数据丢失防护工具中，发现（查找本地硬盘上的敏感信息）和 USB 监控/阻塞是最重要的两个功能。帮助跟踪用户在受认可的企业应用程序之外获取敏感信息，和在本地存储或共享敏感信息的行为也是终端数据丢失防护的重要特征。一旦启用终端发现，选择增量扫描（如果你的产品提供了该功能）；没有人希望他们的电脑因为每周三午间的杀毒扫描而突然停止，而每周四又进行数据丢失防护扫描。同时确保你扫描的位置不只是用户的默认文件目录，因为他们很少会把所有文件放在同一个位置。最后，

如果你允许用户使用本地的微软 Outlook PST 文件，确保你的产品可以扫描 PST 格式的内部去捕获移动到本地存储的邮件。

5. 慢慢来，逐步推出代理和策略。在完成你的初步测试后，一个组一个组的推出那些策略来确保产品具有良好适用性，这样以来不会给你的事件响应团队造成太大压力。当用户第一次开始使用数据丢失防护时，几乎每一个 DLP 客户都会出现大量的策略违反报告，直到用户自我训练到可以更好地管理受保护的信息之时这一情况才会得到缓解。这个过程应该如下：在一个小的用户组中执行一个策略，然后扩大这个策略（和代理安装）持到达到你设定的覆盖范围。一旦第一个策略工作良好，用同样的方式推出第二个策略，虽然你现在不必担心安装新的代理。

虽然这些提示不是部署和管理终端数据丢失防护的所有方面，但仍有助于避免一些最严重的缺陷，并更快的实现你的新工具带来的安全价值。

（作者：Rich Mogull　译者：师成　来源：TechTarget 中国）

怎样箍紧终端安全的“木桶”

相对于弥补短板，现代企业终端安全首先要考虑的是如何把“安全木桶箍紧”，成为一个真正高效的联动体系。

散落的木板

在信息安全领域，最著名的一个定律就是“木桶理论”。它之所以广为流传，很重要的一个原因就是其浅显易懂，然而，易懂并不等于易做，在经过了多年的努力，在绝大多数企业都“听话地”装上了防病毒软件和防火墙之后，人们尴尬地发现，安全威胁和安全事件有增无减，那个传说中牢不可破的“木桶”似乎只能存在于想象之中。

究其原因我们会发现，问题并不在于理论本身，而是其实现的步骤与方法，很多企业过多地将精力投注于弥补和增加所谓的“短板”——更换性能更快、更高的防火墙、增加反垃圾邮件、IPS、上网行为管理等新设备。然而，他们却忽视了一个更为重要的环节，那就是这些“木板”是否真正组成了一个木桶，或者说即使勉强组成，但木板之间有没有较大的缝隙。显然，松散的木桶所造成的泄露，比某块“短板”要严重得多，而对于这一问题的关注，才更能体现我们建立安全“木桶体系”的初衷。

今天的安全威胁正日益变得花样百出，而经济利益的驱使，又使得这些威胁越来越多地趋于隐藏自己，这些无孔不入的安全威胁对企业业务造成的安全挑战，在终端领域表现得淋漓尽致。怎样将针对服务器、PC、移动设备等不同终端、不同威胁的各种防护产品与措施有机地结合起来，控制企业风险、提高应用效率、降低运维成本，所有这些问题的答案，其实质就是寻找一个“能够将松散的木板箍成牢固木桶”的方法，这就是——终端安全标准化解决方案。

终端安全的变革

终端安全从提出到现在，在概念上已经经历了很大的变化，从最初是指安装在电脑上的反病毒软件，到后来的包括台式机、笔记本电脑、移动设备的安全防护，再到以网络为中心的访问控制管理，强调所有联网设备的安全，符合企业安全策略所定制的标准，保护网络免受病毒、木马的侵害。

今天，端点安全已经有了前所未有的充实和完善，其内容已经涵盖了设置管理、防病毒、防入侵、防火墙、主动防御、法规遵从等多种功能。其最终的目的，就是帮助企业防范已知威胁和未知威胁，并且能够在访问公司资产的笔记本电脑、台式机、服务器和移动设备上强制实施安全策略。像防病毒、反间谍软件、防火墙、入侵防御和设备控制这样的端点防护技术与独

立于网络的访问控制技术相结合，可以将安全防护的“木板”有机地结合在一起，从而为系统和网络提供最佳的安全性。

当然，这个听起来简单的目标在实现上需要毫不妥协的严格标准。举例来说，今天的企业往往具备众多的分支机构、合作伙伴以及客户等，不管他们的终端设备以何种方式与企业的网络相连，终端安全系统都应该能够发现并评估端点遵从状态（是否安装了反病毒软件并正在运行、是否及时更新补丁等），设置适当的网络访问权限，并根据需要提供补救功能，同时还应持续监视端点以了解遵从状态是否发生了变化，从而最终在潜移默化中营造出安全、高效的网络应用环境。

困局与转变

在明确了目标之后，企业最先要做的，就是正视自身在终端安全上所陷入的困局，并从中找到可行的转变与出路。

概括来看，目前企业在终端安全领域碰到的挑战主要来自以下几个方面：

1. 从设备层面上，终端往往数量众多，而且规格、配置各不相同，不同终端用户的操作水平和习惯也大相径庭。怎样才能进行有效的管理？

2. 从风险管理和成本控制来看，由于终端是企业应用最活跃的第一线，企业往往需要为保护终端安全不断采购新的产品。怎样在加强风险管理的同时，控制采购和运维成本，提高企业的投资回报率？

3. 从管理运维的难度来看，由于终端设备需要应对花样翻新的病毒、木马、蠕虫的攻击，需要不断采用新的防护技术和设备。怎样让不同的产品设备实现集中的管理和联动？

4. 从终端用户的体验来看，一方面害怕病毒等安全威胁造成的宕机、资料丢失，一方面又担心不断增加的安全软件代理导致终端运行缓慢、性能下降。安全和效率二者成为难以调和的矛盾。

要走出上述的困局，企业的终端安全必须实现四个转变，即由原来单功能产品的松散组合到统一方案集成多种保护技术；从自觉自愿的安全转变为强制统一的安全；从以安全防护为中心转变到以策略遵从为核心；从个性化人工管理转变到标准化自动管理。

终端安全标准化的过程，实际上就是将散落的木板修整并箍紧的过程，这不仅是企业走出终端安全困局的出路，也是企业安全有序化、体系化的必经之路。只有实现标准化，终端安全

的全面防护、统一管理、降低成本、强制安全等所有这些目标才真正能够触手可及，而那个想象中牢不可破的“安全木桶”也才真正有可能成为现实。

（来源：TechTarget 中国）