
# 移动设备安全

# 移动设备安全

随着技术的日新月异，移动设备正逐渐担当着越来越重要的角色，新的移动技术和像 iPhone 具有 Wi-Fi 功能产品的广泛使用可能为新的攻击类型敞开门户——网络犯罪正通过移动设备靠近你……

## 移动设备的安全威胁

在 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。

- 移动恶意软件的威胁：真实存在还是夸大其词？
- USB 会威胁到内置移动设备的安全吗？

## 移动支付风险

移动付款被吹捧为最简单的、最方便的资金交换方式，通过移动付款几乎在任何地方都能以电子支付的方式进行购物和支付账单。用户只需单击一下移动设备的按钮或者在销售网点系统附近晃动一下移动设备，就可以进行购物或者支付账单。这对于购买者来说，支付和购物方便了很多；但是它却给提供这个服务的金融机构引入了很大的风险。

- 移动支付方式的应用风险

## 移动设备风险防御策略

随着智能手机的功能越来越强大并且能够提供类似于台式电脑和笔记本电脑的功能，针对移动设备的恶意软件也在增长就不足为奇了。但是，对于安全专业人员来说，这意味着要保护这些设备不受新出现的移动病毒、蠕虫和间谍软件等传统的恶意软件以及针对移动的垃圾邮件的影响。

- 移动设备网络防御战略
- 智能手机移动设备面临的安全威胁及应对策略

## 保护企业移动设备安全

企业移动设备安全的防护工作不容忽视，虽然有些公司会让技术人员在客户端机器上锁定 USB 端口，限定 CD 为只读，但是，大部分的企业还是依靠软件的解决方式，来管理这些潜在的数据泄露问题。让我们来看看有哪些具体的安全解决方案适用于你企业中的移动设备：

- 如何锁定移动设备 确保企业数据安全
- 企业杀毒软件应考虑移动安全解决方案
- 移动设备之企业安全策略

# 移动恶意软件的威胁：真实存在还是夸大其词？

回顾过去三年，就很容易明白为什么 IT 管理员对厂商们有关移动威胁增长的推测表示怀疑。

去年这个时候，McAfee 称，在参加调查的两百多个运营商中，83%表示曾有过移动电话感染的经历。之后，安全专家发出警告，iPhone 的推出将引发更多的移动攻击。

上个月，安全厂商 Sophos 发布一个报告，警告移动电话使用者面临不断增长的威胁。报告还说，新的移动技术和像 iPhone 具有 Wi-Fi 功能产品的广泛使用可能为新的攻击类型敞开门户。报告补充道，随着个人 Wi-Fi 产品不断受欢迎，随之发生的恶意行为只是迟早的事情。

对于 IT 专业人员而言，移动电话攻击将不断增长的警告已经讲了三年多，但还是没有发生任何重大的事件，自然而然，很难不让他们不产生质疑。

这是否意味着一直以来，移动电话的威胁都是夸大其词，安全厂商过度炒作，制造恐慌，来出售其新产品？并非如此。

的确，企业几乎很少遭到针对移动电话的攻击。但是，那只是因为公司仍然对员工使用该设备的功能有所限制。比如，现在的手机大部分都具有上网的性能。但是，在工作环境中，手机的使用还仅限于通话和收发电子邮件。

“我不知道是否我们真的希望人们使用智能手机，来处理复杂的事情。”Jason Smith 说。他就职于一家 250 名员工的法律公司 Behle & Latimer，是应用软件管理员。Smith 对于移动安全的关心主要是手提电脑的使用。在日常工作中，公司的律师们都使用手提电脑来传递敏感的文件。很多员工都使用 BlackBerry，但是 IT 部门对 BlackBerry 有更多的控制权，能够从服务器端对必要的安全控制进行管理。“对于 BlackBerry，我们可

以锁定该设备，能够加以控制。但是我不想员工使用 iPhone 或者其他智能手机来传递敏感文件，因为我们对此无法控制。”

尽管大多数企业还没有感觉到基于移动电话攻击的紧迫感，但是 Sophos Senior Technology 公司的咨询师 Graham Cluley 和 F-Secure 公司的反病毒研究总监 Mikko Hypponen 对此意识的淡薄发出警告。他们说，智能手机文件共享成为公司的日常惯例，只是时间问题；当这个发生时，麻烦也就接踵而至。

**基于电话的计算仍然局限于企业**

现在，Smith 最后担心的问题才是针对使用智能电话和其他手持计算设备的员工进行的攻击。他知道存在利用恶意软件攻击 BlackBerry 使用者的潜在性，但是事实上，BlackBerry 很容易实现安全加固。“就安全管理而言，我们几乎可以在 BlackBerry 服务器上做任何事情。”他说。

相反，他的移动关心集中在他所在公司不断增长的手提电脑使用。目前公司有二十台手提电脑，员工通常使用手提电脑传递 PDF 和 Word 文件。这里存在的风险在于，如果攻击者能够利用木马或其他恶意软件感染机器，那些机密的法律文件和电子邮件有可能落入攻击者的手中。

同时，他还担心包含敏感数据的手提电脑丢失或被窃。他提到，五年前，有几台公司的手提电脑失踪了。至少有一台遗失在飞机上，另一台在员工家里被偷。虽然没有任何证据显示这些电脑中的敏感数据被用于欺诈行为，但是现在公司不敢再次冒这样的险。远程用户必须通过 Citrix 网关使用多重因素认证登录。公司使用 BioPassword 公司的软件进行验证。

但这并不能确保员工使用的移动电话的安全性。不过，这关系不大。Smith 看到的是未来两年内，手提电脑的使用会大量增加，但智能电话的使用将不会超过目前的功能。他说，如果律师想和同事传递敏感文件，在可预见的未来里，他们应该不会使用智能电话去传递文件。

“那些设备目前主要还倾向电子邮件的用途，”他说，“如果一家公司使用手持设备目的就在于此的话，我建议使用 BlackBerry，因为目前它是最容易支持的。”

**为什么 IT 应该关注**

Cluley 认同，像 Smith 的 IT 专业人员不太可能会为智能手机的威胁而彻夜难眠。正如他所说，移动恶意软件的问题与 Windows PC 每天面对的威胁相比，目前就像“暴风雨中的一点雨滴”。他说，在 PC 方面，出于金融动机的团伙已经采用一种“传送带”哲学原理，即努力开发新的恶意软件，每次稍作修改，让安全工具失效。Sophos 已经看到移动恶意软件领域也有这样的转移。

“随着人们越来越普遍地使用包含个人信息、支持 Wi-Fi 的设备，黑客使用恶意软件的诱惑也会越来越大。” Cluley 说。

他说，iPhone 就是一个未来走势的很好例子，在其移动电子邮件程序和 Safari 浏览器都发现了漏洞。现在，攻击仍然有限，对于寻求更大回报的网络罪犯，是不太可能在不久的将来对此进行大规模的攻击。但是针对 iPhone Web 浏览器漏洞的概念性攻击代码已经公开，随着更多的第三方应用将写入这些设备，在未来发生滥用只是一个时间的问题。

“我认为，在移动恶意软件方面的不久将来，iPhone 和 Google Android 将是很有趣的平台。”他说，“Android 很有意思。是否一个移动电话的开放标准或多或少令移动恶意软件成为一个问题？这里，关键点是是否 Android 将成为全部开放系统，还是将采用诸如 Symbian 的登陆许可应用软件的系统。”

如果未登录或不明的应用程序由某些对电话功能有全部访问权限的人编写的，那么麻烦也将很快来临。

“我已经在 iPhone 上感觉到麻烦问题的到来，”他说，“一个封闭的环境已经创建一个如此活跃的黑客环境，那么，越来越大的可能性就是有人会写一点真正对它不利的东西。”

*（作者：Bill Brenner 译者：Shirley 来源：TechTarget中国）*

## USB会威胁到内置移动设备的安全吗？

**问：**使用USB会威胁到内置设备的安全性吗？特别是当这些设备是通过USB和电脑主机连接的时候，通过使用在电脑主机上运行的应用，这些设备会被入侵吗？

**答：**确实可以。看一下USB设备是如何连接到电脑的，你就明白为什么了。通用串行总线（Universal Serial Bus），也就是通常所说的USB，它是用于把设备连接到电脑主机上的串行总线标准。一条总线就是在电脑之间或者电脑组件只见个传送数据的一个子系统。最为一个串行总线，USB一次发送一位的数据。它的创建是为了改善越来越多的想连接到电脑上的即插即用功能。

在刚使用个人电脑的时候，连接新设备是麻烦的事情。那时必须要设置传输器、增加额外的总线或者并口，安装设备驱动并重启，可能是多次。现在有了USB这种单一的标准界面接口，这些日子就过去了。USB设备可以在不需重启电脑或者关闭设备的情况下连接或者断开。当然，它就被广泛地用于连接接口，根据2008年的USB使用者论坛（USB Implementers Forum）称，目前全球有20亿有线USB设备。但是，USB只是连接到电脑主机的接口设备标准。它并不提供任何安全功能来过滤通过连接的数据。在这一方面，这和以太网或者打印机电缆相同；任何通过USB连接连到电脑的设备都可以被在电脑上运行的应用访问。所以，假如，如果电脑被恶意软件感染了，这些恶意软件就可以访问通过USB线连接到电脑的便携式硬盘上的数据。危险也可以发生在相反的情况，带有自动运行的应用（包括恶意软件）的U3 USB设备连接到一台电脑，然后就可以防火电脑主机上的数据或者记录电脑键盘上的所有字符。

为了减轻这种风险，你可以禁用电脑上的所有USB端口，但是这不太现实，因为这些端口可能被键盘或者鼠标等设备所使用。如果企业运行的是Windows的网络，就可以通过使用Active Directory控制USB设备。不需要使用USN设备的个人和团队，就可以通过Active Directory组策略，禁止访问ubstor.pnf和ubstor.inf文件。在Windows Vista中，管理员可以允许用户只安装在同意列表上的设备，或者禁止可移动或者使用可移动媒体读写访问设备。还有一些第三方程序可以提供USB设备的访问控制范围。

可喜地是我们看到的 USB 还只是把设备连接到电脑的方法，而不是控制设备行为的方式。为了保护 USB 设备，你可能需要一些安全措施，当然，这些措施可以被涵盖的策略支持，并可以清楚地和 USB 设备的恰当使用交流。

*（作者：Michael Cobb 译者：Tina Guo 来源：TechTarget中国）*

## 移动支付方式的应用风险

移动付款被吹捧为最简单的、最方便的资金交换方式，通过移动付款几乎在任何地方都能以电子支付的方式进行购物和支付账单。用户只需单击一下移动设备的按钮或者在销售网点系统附近晃动一下移动设备，就可以进行购物或者支付账单。这对于购买者来说，支付和购物方便了很多；但是它却给提供这个服务的金融机构引入了很大的风险。

这不是移动银行业务第一次亮相了。几年前，在向电子货币和数字身份证转变的第二个革命性阶段就出现了移动付款的身影。那时移动付款业务的发展受到技术限制和高成本的困扰，不论是消费者还是服务提供商都面临这些方面的问题。无线应用协议（WAP1.0）的普及遭遇了很大的挫折，因为移动设备和移动业务服务提供商之间存在着巨大安全缺口，这一情况被叫做“WAP 缺口”。

今天，很多过去的技术限制和安全顾虑都已降低了，而移动付款业务利用这些技术上的进步又一次浮出了水面。其中一个重要的变化是 WAP 2.0 的使用，它允许在移动设备和服务提供商之间进行端到端的加密。

但是移动付款业务还是存在风险，金融机构采用移动付款程序之前，他们应该考虑以下几个关键的风险区域：

**第三方供应商：**移动付款服务提供商建立了一个机制，可以让用户把他们存在银行帐户或其它受监管的金融企业中的货币取出来。这些服务提供商是财务中间人，他们提供的服务被列为货币服务业务（MSBs）。货币服务业务提供商必须遵守与其合作的州内的法律。然而，不是所有的州都有监管 MSB 活动的法律，所以在选择的过程中应该仔细审查。如果你所在的财务公司决定使用 MSB 进行移动付款交易活动，那么请务必检查 MSB 提供商实际的信息安全情况，从而让自己放心。

**监管和法律责任：**美国现在几乎没有能够防止移动付款业务被滥用的安全措施。安全措施的规划和宣传指导方面几乎没有进步，传统的洗钱对策不能充分地处理因移动付款滥用引发的电子银行和无现金服务系统威胁。到现在为止，几乎没有任何基金会去研究和发展法律，从而执行现有的几个监管规则。金融机构必须让他们的法律团队和规则遵从团队制定使用移动付款系统的“交通规则（rules of the road）”。规则应该包括全面的 MSB 服务提供商实际安全情

况审查，全面的支付卡行业数据安全标准(PCI DSS)的遵守情况审查，以及制定一个强有力的涵盖突发事件应对和责任的合同。另外，如果一个金融机构参加了政治活动团体，则一定要教育和告知团体的代表们，让他们清楚为客户开发相关法律和安全措施的必要性。

**预防欺诈/损失的措施：**金融机构必须能够监视和跟踪可疑的交易活动，这就要求交易活动对金融机构是透明的，以便于其收集情报。这有时候需要得到政府情报机关和政府执法机构的协助。不幸的是，这些组织在移动付款技术方面几乎没有专业的技能。很多国家在通过移动电话进行货币转移领域没有相关的法律和监管政策。移动电话网络有一些安全功能，可以阻止执法部门和情报服务部门检测可疑的非法交易。迅速发展的技术能力正超过政府追踪货币交易的能力，甚至会使金融机构不必再遵守美国爱国者法案（USA Patriot Act）和银行保密法（Bank Secrecy Act）。

由于无线环境中安全威胁的属性和数量的不确定性，金融机构应该对他们的移动付款系统实行独立的、阶段性的安全漏洞评估，评估的重点放在那些能够识别可疑交易活动或者可疑付款活动的检测系统和反馈系统，这项工作非常的关键。另外，金融机构必须命令他们的第三方付款服务提供商也要进行评估，以便于他们进行审查。这些评估应该在每一次大的环境条件改变时进行。移动付款欺诈处理程序应该有利于对检测到的威胁和滥用展开迅速调查以解除威胁。这将帮助执法部门和政府情报机构在必要的情况下对你的企业进行协助。

总体而言，虽然移动付款业务在电子付款的可行性和安全方面已经有了一些显著的改进，但对于金融机构来说，现在采用这个服务还是有几个大的风险。随着培训和安全措施的改进，以及技术在市场上变得司空见惯，一定会浮现出新的风险和威胁来挑战今天的安全改进。移动付款可以更快、更方便、障碍更少，但是这些对于攻击者来说也是如此。金融机构必须权衡风险和利益，然后决定现在时机是否适当，能否出手一搏。

*（作者：Rick Lawhorn　译者：Sean 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)*

# 智能手机移动设备面临的安全威胁及应对策略

如今，许多公司的 IT 部门需要做这样一项工作：使工作人员能在掌上电脑（PDAs）或者智能手机这类的无线手持设备上处理商业数据。在理想的情况下，所有的这些设备都是值得信赖的，并且不受恶意软件的干扰。可现实的情况是，许多设备都处于无人管理也没有安全保障的状态，这就成为手机恶意软件感染的理想目标。企业如何才能在这些问题泛滥前，将潜在的风险遏制在萌芽状态呢？

**智能手机和掌上电脑的安全威胁日益增加**

和 Win32 平台上的情况相比，手机恶意软件的数量仍然很少。迄今为止，已被发现的、专门针对移动操作系统的病毒、蠕虫和特洛伊木马不到 500 例。大多数只造成相对较小的损害，诸如：文件丢失、硬件重置或产生额外的话费。

不幸的是，长期制约恶意攻击的门槛正渐渐消失。首先，移动设备的使用人数正飞快增长。其次，新型热门商用消费级终端设备（如苹果公司的 iPhone 和 HTC 公司的 Android G1）的市场可能最终会发展成一个利润丰厚的市场，吸引到大量恶意软件开发者。

此外，现代智能手机已不再受制于狭窄的无线覆盖范围、单一化的操作系统或兆级别的存储容量。近乎无处不在的 3G 及 Wi-Fi 简化了恶意软件的无线传播，而数 G 字节的存储容量使得更多的敏感数据会被窃取。随着用户越来越多地通过移动设备使用电子邮件和上网冲浪这些应用（这也是传统恶意软件的传播媒介），这使得恶意软件的传播变得更加可行。而短信服务（SMS）和多媒体信息服务（MMS）也成为传播恶意软件的新方式。

最后消失的一道门槛可能是：那种容易让攻击者妥协的单一的移动开发环境。在过去，各种不同规格、封闭的开发环境常常使恶意软件无从下手。而塞班软件公司 Symbian Software Ltd. Series 60 系统则因开发环境友好，成为被攻击次数最多的移动平台。如今，Android 和 Linux 正建立起开放的系统开发平台。那些存在于 MacOS 和 Win32 环境中的恶意软件，也有可能入侵 iPhone 和 Windows 的移动开发平台。

**智能手机和 PDA 安全软件**

幸运的是，随着移动设备变得更加强大，移动操作系统的安全模式以及第三方的安全程序也得到了发展。移动智能手机和 PDAs 的管理者可以安装上这些现成的防御软件来检测和阻止移动恶意软件的安装和执行。

**首先，**可以通过检查所有移动设备的可执行文件和安装文件的数字签名。这些数字签名包括塞班（Symbian）或微软 Mobile2Market 签署的认证程序，以及 Research In Motion 公司针对黑莓的控制 APIs。通过使用像黑莓企业服务器或 Sybase 公司的 Afaria iAnywhere 这一类的移动设备管理工具来管理安装文件，可以帮助用户防范移动恶意软件的自动安装。另外，可以创建移动软件白名单和黑名单，教会用户如何避免运行未签名代码，并明白这样做的原因。

**下一步，**利用移动操作系统的访问控制，阻止恶意软件篡改文件和调用敏感功能。例如，塞班 9 的权限管理政策可以限制程序访问系统和/或用户的文件及网络接口，而数据锁定可以把数据划分到私人文件夹里，并对不受信任的程序不可见。配置这些访问控制策略有利于阻止间谍软件窃取数据，防止特洛伊木马留下后门。

**最后，**不同于笔记本电脑的是，移动手持设备没有在出厂时安装防火墙、杀毒软件或垃圾邮件过滤器。可以考虑通过安装常驻于系统的移动安全程序设备来填补这些空缺。例如，适用于一般的移动操作系统的防病毒和 SMS 垃圾邮件的程序（这些移动操作系统厂商包括 AirScanner、F-Secure、McAfee、赛门铁克、SMobile 系统、趋势科技和 Sophos 等公司）。这些程序精于处理移动设备的威胁，如检测移动操作系统的特洛伊木马、过滤短信，阻止恶意软件入侵企业服务器。

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

# 如何锁定移动设备 确保企业数据安全

尽管企业和厂商都对通过 Email 或网络造成的数据泄露相当重视，但事实是，敏感的公司数据更有可能通过丢失的手提电脑、CD 盘或 USB 盘落入他人手中。以下就是几个真实发生的实例：

1.2006 年五月份，美国退伍军人事务部门透露，一台包括两千六百万名退伍军人个人信息的手提电脑失踪。信息实际上是保存在一个移动硬盘上。

2.2007 年十月份，英国税务海关总署丢失两张 CD 盘，包括两千五百万名英国公民的财务记录。

3.2006 年二月份，一名德勤会计公司（Deloitte & Touche）的员工将一张包括 9290 名 McAfee 公司员工信息的 CD 盘遗忘在一家航空公司的座位后面。

4.2007 年，报告显示，包括敏感军方信息的 USB 盘在阿富汗的街头售卖。

对手提电脑可以采用全磁盘加密（full-disk encryption），但是，可移动设备却带来更多的挑战。移动办公的员工在出差时，有合法的需求需要使用这样的设备来传输数据，甚至敏感数据。以前曾有专用的硬件用于此用途，但价格下跌幅度太大，现在甚至在一个会展上，容量上兆的 U 盘都免费赠送，而且，如今也很难发现一台手提电脑不跟配 CD 或者 DVD 光驱。

虽然仍然有些公司会让技术人员在客户端机器上锁定 USB 端口，限定 CD 为只读，但是，大部分的企业还是依靠软件的解决方式，来管理这些潜在的数据泄露问题。让我们来看一下几个软件解决方案:

1. 在 Windows XP 和 Vista，可以利用组策略对象(GPO)限制设备的安装。Vista 提供的策略比 XP 更加细化，但是，已经由用户安装好的设备可能仍然还是可用，这要看组策略对象是怎么配置的。这个是免费提供的，但其灵活性可能不如其他解决方案，还有提供的安全性也有限。
2. 许多第三方的软件工具能够限制移动存储的使用，包括 CD-ROM 和 USB 设备。策略可以非常细粒度，只有公司批准的设备才能访问，连接数码相机和音乐播放器只允许只读，而同时仍然可以阻止来自外部的数据传输。多数工具支持基于角色和系统的策略，允许对不同的用户和电脑组规定不同的限制（例如，所有的台式电脑完全禁用写入访问，但高层的手提可以启用）。

3. 阻止或审计对移动存储访问的第三方软件。策略允许访问，但同时保留一份这些文件的安全备份，然后，在下一次手提电脑连接到公司网络时，发送到管理服务器。这样，管理员就可以审阅活动，包括文件的内容，以判断是否符合公司政策。
4. 对移动存储进行可选或必选数据加密的加密软件。用户可以在公司和组密钥或者选择带密码的自身解密归档进行选择（视策略而定），来传送给不使用同一加密软件的合作伙伴。有的工具可以基于用户、组、系统或者存储设备实行策略。
5. 符合集中策略的专用 USB 设备。这恐怕是最贵的选择，不提供任何优于软件解决方案的实际安全好处。
6. 具有终端保护的数据丢失防护（DLP）产品。这些工具能够基于被检测的内容应用动态的策略。例如，可以对一个包括信用卡号码的文件加以限制，但是不包括敏感内容的 PPT 就可以进行传送。最好的工具使用深层内容分析，不仅仅保护易于识别的内容，例如信用卡号码、银行帐号，而且还保护半结构化数据，如被保护文件的一部分。有些工具包括加密，或者使用合作方的加密。DLP 是具灵活性的选择方案，所有工具都将最终包括基于内容的能力。不过，他们定义策略更为复杂，成熟程度的差异不均。

企业有多种方案可以选择，从简单的阻止设备的使用到实时的、与动态加密相连、基于内容的策略。最适合贵公司的解决方案要视公司的具体需求、用户的接受程度、预算和现有的基础设施而定。

*（作者：Rich Mogull 译者：Shirley 来源：TechTarget中国）*

# 企业杀毒软件应考虑移动安全解决方案

杀毒软件是目前企业环境中最重要的一种应用程序。因此，在智能手机、掌上电脑和其它移动设备集成到标准的商业行为中的时候，迫切地需要保护它们就一点也不令人感到意外了。移动设备担当了日益重要的角色，让信息工作者连接到企业网络以及互联网。但是，对于安全专业人员来说，这意味着要保护这些设备不受新出现的移动病毒、蠕虫和间谍软件等传统的恶意软件以及针对移动的垃圾邮件的影响。针对移动设备的垃圾邮件有时候称作“SPIN”。

据市场研究公司 Gartner 称，到 2009 年，智能手机销售量将占全部手机销售量的比例将从 2004 年的不到 3%提高到 27%。随着智能手机的功能越来越强大并且能够提供类似于台式电脑和笔记本电脑的功能，针对移动设备的恶意软件也在增长就不足为奇了。

**多种平台**

智能手机经常是通过雇员自己购买设备进入企业的。然后，他们要求 IT 部门允许他们使用自己的设备做公司的事情。在企业制定出全面实行标准化的决策之前，IT 部门设法寻找一个能够支持运行 Symbian、微软、Palm、Linux 或者 BlackBerry 操作系统的各种设备的解决方案。

同有线领域一样，移动恶意软件喜欢感染一种特定的操作系统。在无线领域，平台的选择到目前为止一直是 Symbian 操作系统。这个操作系统声称占移动手机市场份额的 75%以上。随着微软的市场份额达到了 17%，大多数企业移动杀毒软件产品都包含了对 Symbian 和微软操作系统的支持。在企业中流行的 Blackberry 设备到目前为止还没有看到移动恶意软件。

有许多方法可以解决保护企业中各种平台和设备的问题。首先是实现一个机构内部的操作系统或者设备的标准化，尽管这并不总是很容易的。遗憾的是许多智能手机和掌上电脑是“用户配置的”，这意味着用户首先购买，然后要求与企业网络实现同步，几乎没有看考虑到安全问题。

解决不同种类移动设备的另一种方法是寻找移动杀毒产品，因为许多厂商提供的产品都是要保护多种操作系统的。

### 部署和更新

随着智能手机和掌上电脑(实际上就是微型计算机)连接到企业网络访问从电子邮件到 CRM 应用软件的一切东西，企业不能承受这些设备受到恶意软件的攻击。然而，在部署移动安全软件的时候有一个明显的难题，特别是在一个企业拥有在全球环境中使用的数千台不同的设备的时候。即使在软件已经安装到这个设备上的时候，IT 管理员仍需要一种方法管理更新和访问记录。

在选择一个移动杀毒解决方案的时候，应该考察这个产品如何能够方便地结合到你目前的基础设施中。遗憾的是，企业移动设备安全产品仍然很新，到目前为止还没有完全集成到行业巨头的杀毒套装软件中。例如，尽管其移动产品还不是其许可证销售目标的一部分，赛门铁克杀毒软件产品中的系统中心管理控制台仍向管理员提供了对所有运行移动安全企业版软件的智能手机进行整个企业范围内的控制。

不过，还有其它的类似于趋势科技的移动安全软件的产品要与现有的设备管理软件配合使用，如 Akamai 技术公司和 iAnywhere 解决方案公司的 Afaria 系列产品。根据你的机构现有的杀毒产品，可以通过各种方式增加移动保护，如下载免费的软件根据需要进行安装和增加能够提供集中管理的集成产品的安全预算等。

移动安全产品还没有成为一种标准的企业应用程序，许多厂商现在都没有把在安全套装软件许可证中包含移动产品，因为这些许可证的覆盖范围不同。

一旦移动安全产品安装到设备上，访问软件更新是同样重要的。移动设备有许多方法进行更新。理想的方法是通过集成的安全控制台。所有的企业杀毒软件更新都是通过这个控制台发布的。

然而，由于有多种提供方式，移动设备增加的额外范围超过了传统的 IP 网络。例如，F-Secure 公司的移动安全产品能够在一个 HTTPS 数据线路上自动更新特征库，通过短信逐步更新，或者通过 GPRS 线路在后台更新。

### 杀毒以外的功能

纵深防御是任何 IT 安全管理员常说的话，移动设备也不例外。在企业应用移动设备时引起麻烦的并不仅仅是病毒。在移动领域，垃圾信息给企业带来了巨大的财务负担。与传统的垃圾邮件不同，当移动设备接收到垃圾信息时，其成本不仅包括企业消耗的带宽，而且还包括删

除这些垃圾信息所耗费的时间。随着运营商对每一条短信/彩信在线消耗的时间和数据传输进行收费，垃圾信息很快将给企业增加额外的成本。

而且，随着移动 VoIP 技术取得进展，企业将不得不应付文本垃圾信息以外的现实。安全厂商已经开始准备应付语音垃圾信息的出现。语音垃圾信息是采用 VoIP 技术产生的廉价的自动电话。

这是单一的杀毒产品在当前的移动安全企业领域不能起作用的一个原因。厂商已经认识到解决当前部署移动设备的需求问题不仅仅是把现有的杀毒产品移植到移动环境中。

要覆盖所有这些基础，你们应该寻找一些把反垃圾信息、反间谍软件和个人防火墙功能集成到他们的产品中的移动安全解决方案。

**透明度**

在选择一种企业移动安全解决方案的时候，必须要考虑可用性和效率。趋势科技移动设备安全经理 Todd Theimann 强调指出，移动安全产品对于用户来说应该是无缝的。否则，企业就会冒用户绕过安全措施的风险。因为用户可以关闭安全软件或者在设备本身进行厂家重新设置。

运营商还认识到移动设备安全的普遍需求并且已经开始把杀毒和反垃圾信息功能包含在其服务合同中。虽然这有助于缓解移动恶意软件攻击的可能性，但是，这并不是向企业部署提供移动安全的总体解决方案。

*（作者：Sandra Kay Miller　来源：TechTarget中国）*

# 移动设备之企业安全策略

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)*