 随着信息技术的发展，越来越多的企业正在逐步完善业务流程及信息处理，将其从人工操作转移到信息协作平台上来。因为Windows操作系统易于使用、成本较低，许多企业把Windows作为主要的业务流程和信息处理平台，从边界服务器到内部网络，从企业总部到各分支机构，企业中存在大量使用Windows操作系统的服务器和客户端，它们的广泛使用，也随之出现了层出不穷的安全威胁，各种入侵攻击事件时常见诸媒体，其中更有不少造成严重的经济损失，面对如此严峻的安全形势，企业用户应当如何应对? 针对这样安全形势，微软推出了ForeFront Security安全产品家族，其中包括ForeFront Client Security、ForeFront Server Security 和ForeFront Edge Security，范围涵盖了客户端、服务器和网络边界安全。和原来的单点安全产品(只面向某一个平台的安全产品)相比，新的ForeFront家族更注重整体安全这一观点，讲究从整体架构上来保证用户信息平台的安全，同时ForeFront也更关注企业安全管理的实施。从这点上讲，ForeFront可以说是体现了Microsoft对企业用户的Windows操作系统和网络安全需求的理解，下图取自ForeFront Security的Microsoft官方站点，读者从中可以很直观的了解ForeFront家族的成员组成。 ForeFront Security的特性 ForeFront Security不单只有以ForeFront Security命名的几个产品，它还包括了众多的Microsoft 安全产品，比如WSUS、System Center、ISA、IAG等。所谓“ 透过现象看本质 ”，虽然ForeFront的产品

线相当复杂，不过我们仍可看到Microsoft在 ForeFront上所要实现的三个特性：综合、集成、简易 ●综合(Comprehensive) ForeFront家族是客户端、服务器和网络边界安全的完整解决方案，包括了恶意软件防御、补丁管理、身份验证、远程访问等安全功能，保护范围覆盖企业网络和所有采用Windows操作系统的节点。 ●集成(Integrated) ForeFront可以和用户现有的Windows平台上的信息处理体系和安全方案紧密的集成在一起，使用户可以更有效和更清楚的控制企业网络中的安全情况。 ●简易(Simplified) ForeFront给用户提供了单一的管理视图，增加用户对企业网络安全状态的可见性，从而可以实现更好的管理和威胁缓解过程。 企业用户从ForeFront的三个特性中可以得到什么启示呢?让不同行业不同大小的企业来回答这个问题会有不同的答案，但笔者认为答案的区别应该是在这三个特性的优先度排列上而不是在答案的内容上。因为ForeFront Security的一些组件尚未正式推出，现在从整体安全架构的技术层面上，来讨论ForeFront与其它安全方案的优劣，似乎尚早，不过从 ForeFront的设计理念上来讨论一下Windows平台安全的实现，倒是个相当有启发性的话题。 Forefront与企业安全四特性 安全综合性首先是Windows安全实现的综合性。目前大部分的企业中原有的安全实现可以归类于“ 头痛医头，脚疼医脚 ”式的方案：如果客户端时常面临恶意软件的威胁，企业的信息部门会购买单机版的反病毒软件并安装.如果服务器有可能遭受黑客入侵，企业的信息部门会购买防火墙，安装入侵检查设备.如果邮件服务在某一时段内有大量的垃圾邮件侵袭，企业的信息部门会购买各种反垃圾邮件的安全产品企业对安全方案的采购和部署并不是基

于对影响企业业务和信息处理的安全威胁的战略性分析，而只是为了防御某类型的安全威胁而进行的短期行为。这样的采购和部署思路虽然在短期内有不错的效果，却会给企业带来虚假的安全感和不小的安全隐患，企业往往在日后遭受到新安全威胁的损害之后，才会对认识新威胁并对其做出反应。www. Examda.CoM考试就到百考试题 最近频繁出现在媒体上的0Day漏洞攻击便是一个例子，企业如果只部署了一般的反病毒软件和防火墙(这样的企业环境很常见，为简便起见，下文称为一般信息处理环境)，在0Day漏洞的攻击下是毫无防御能力的，唯有在同时启用入侵检测、反病毒、防火墙等安全功能的情况下，才能比较有效的检测和拦截。此外，企业缺乏远见的安全方案采购部署方法，也很容易导致安全功能的缺失，进而在企业的信息安全体系中造成潜在的弱点。一个桶能装的水取决于最短的桶板的长度，一个缺乏某些关键安全功能的安全体系，实际的安全效能并不比什么安全方案都不用的环境安全多少，还是用上面提到的一般企业信息处理环境做示例，如果不在内部网络中使用WSUS服务或使用Windows Update，管理员无法掌握每个网络节点的补丁升级情况，一个利用Windows漏洞传播、反病毒软件暂时无法检测出来的新蠕虫将可以很轻易的攻陷企业内网的所有机器。从这个角度上讲，企业用户要实现Windows平台的安全最大化，贯彻Microsoft 在ForeFront Security中所要实现的“ 安全功能的完整性 ”这一理念就显得无比重要。来源：考试大的美女编辑们 安全集成性 其次是Windows安全实现的集成。ForeFront Security就强调了其安全功能和用户旧有的Windows平台应用的无缝结合。企业信息处理环境的组成

非常复杂，即便在稍微上点规模的企业中，信息处理环境就可以按照信息处理需求的不同分为各种应用服务器、关键网络服务器、客户端机器等多个环境类型，更不用说大中型的企业或跨国企业。而各个环境上的软硬件环境又是千差万别，安全级别和性能需求也是各不相同，例如，企业要在应用服务器上部署一套负责内容过滤和性能监控的安全方案、可是事先又没有对待部署方案与旧有的应用服务器环境的兼容性和整合性进行过严格测试，只凭广告的宣传进行选择，那后续的故障排查对企业信息部门来说无异于一场噩梦，这套安全方案的实施效果也无从谈起。因此，企业在部署安全方案时，无论是从实施效果还是保护原有投资的角度来说，安全方案和旧有设施的集成性都是必须考虑的关键因素。来源：www.examda.com 安全简易性最后是安全实现的简易性，也称为可操作性。根据心理学的解释，越是关键的决定或操作，过程应该复杂一点，给操作者反复检查和确认的机会，减少出错的可能. 而越是频繁的动作，过程越是应该简单一点，最好能把多个简单的动作合而为一。管理员对企业网络中的各Windows节点、应用服务器和网络设备的监控管理属于日常行为，操作理应简单一点。但因为目前企业中缺乏完善的管理方案，许多企业中仍采用服务器由信息部门集中管理，客户端由用户自主管理的分散式管理方法。在大中型企业中常常会看到这样的情况，每到Windows系统进行补丁升级的日子，信息部门就需要处理大量的服务器和客户端，耗费的人力惊人，而且从补丁发布到整个企业的系统完全更新也成为企业网络最容易受到攻击的时间段。信息部门也无法获得Windows客户端上的警报和日志信息，即使是对集中管理

的服务器上发生的安全事件反应也相当滞后，信息部门疲于奔命于各种安全警报的处理。 Forefront安全架构的推出，无疑为企业Windows架构的管理带来了令人振奋的消息。来源：考试大 安全变更性 企业的IT管理中还有一个非常重要的方面变更控制(Change Control)。信息部门需要掌握企业网络中每一次变化，以便于故障排查和追踪。这些变化包括安全策略的变更，服务及应用的变更，软、硬件环境的变更，甚至于管理组织的变更。这些变更对于大型企业来说，随时随地都在发生着，其数量之大令人咋舌，那么如何评估、监控、取证及完善这些变更，是每个企业IT主管的恶梦。例如，用户在客户端上私自进行企业安全策略不允许的操作或软件安装，往往会给企业网络的安全埋下隐患，这两年频繁出现在新闻中的，通过移动存储设备传播的各种恶意软件以及ARP病毒，就是没有有效控制客户端，违反安全策略的行为，最终导致安全事故的例子。对于这一点，Forefront安全架构利用自身的安全特性，并结合System Center产品系列，很好的实现了企业IT安全管理的目标。 用ForeFront保障安全 综上所述，一个安全解决方案至少需要考虑到四个方面：综合性、集成性、简便性和变更性。就此而言，ForeFront Security是个不错的选择。但不是说在企业中实施了Forefront，就实现了企业IT安全了，一方面，安全管理更多的是对人对流程的管理，另一方面，刚上市的产品也需要时间逐步进行完善。企业在选择方案时，首先对自己的业务流程、IT设施和面临的安全威胁进行详细的分析调查，对前面提到的四个要求进行优先度排序，然后在ForeFront家族中，根据自身的情况，选择合适的产品组合。 编辑特别推荐: 右键菜单快速整

理Windows7磁盘碎片 Windows安全性饱受质疑 Windows虚拟内存详解 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com