高性能企业级系统及安全管理

——BigFix 统一管理平台

目 录

1 前言 1

2 IT 部门的职责 1

3 BIGFIX 平台 2

3.1 分布式可视及管理神经系统 3
3.2 BIGFIX 代理 4
3.3 BIGFIX 服务器和控制台 6
3.4 BIGFIX FIXLET 消息 7
3.5 BIGFIX 中继器 7

4 BIGFIX 解决方案 8

4.1 BIGFIX 系统生命周期管理 8
4.1.1 资产/License 管理 8
4.1.2 软件分发 9
4.1.3 补丁管理 10
4.1.4 电源管理 11
4.1.5 远程协助 11
4.2 BIGFIX 安全配置和漏洞管理 12
4.2.1 安全配置管理 13
4.2.2 漏洞评估 14
4.3 BIGFIX 终端防护 14
4.3.1 防病毒 15
4.3.2 终端防火墙 15
4.3.3 反间谍软件 16
4.3.4 第三方防病毒软件客户端管理 16
4.3.5 网络准入控制 17

5 部署与使用 18

6 BIGFIX 产品特点及优势 19

6.1 实时可见及可控 19
6.2 整合与控制 19
6.3 单一可信来源 19
6.4 卓越的可扩展能力 20
6.5 最小客户端资源占用 20
6.6 可靠的系统安全性 20
6.7 可视化管理 21
6.8 全面的解决方案 21

6.9 强大的定制能力 21
6.10 先进的离线管理能力 22
7 公司介绍 22

1 前言

近年来，企业一直在以超乎想象的速度高速运转。复杂和高分布环境的持续增长支撑着由合作伙伴、供应商，分销商和顾客组成的错综复杂的网络。随着企业利用技术实现创新和提供新的服务的愿望越来越迫切，面向服务的架构和基于Web的应用发展已经从构想转化为真实世界的实际应用。在这个全新的世界中，对于顾客、供应商、员工、监管机构，投资人和其它相关机构来说，IT部门提供的服务必须是7 x 24小时可用的。

同时，IT 基础架构极高的暴露率正在从根本上改变着企业对 IT 资产，过程及数据的管理方式。IT 组织不再将资源管理及维护工作视为可按照自身选定的时间和条件执行的后台功能，其工作也不再是免受外部审议的内部事务。IT 管理过程的成败与否原先很大程度上只是组织内部的考核目标，但现在更多以企业运营是否成功，是否实现法规遵从或企业是否具备执行力等作为判断的标准。

要满足这些要求，IT 组织迫切需要迁移到新的 IT 安全和系统管理平台。新的平台模型可在整合及降低基础架构管理成本的同时不断地从根本上提高企业对可控制 IT 资产和数据的实时阅读能力。一直以来，所谓“少花钱，多办事”更多是一种妥协的方法，但在变革 IT 基础架构的管理的过程中，新的管理平台却可以使其成为提升管理水平和创造价值的有效途径。

2 IT 部门的职责

IT 部门在帮助企业成功方面肩负着以下三种主要的职责。首先，必须保证所有的 IT 系统和网络被管理并经过优化，可以以最低的成本贡献最大的商业价值。其次，必须保护重要的基础架构不受到日益严峻的敌对威胁环境的侵害——包括间谍软件、病毒、攻击，入侵和人为的安全失误等。第三，必须防止违反法律或由于违背法规遵从而受到处罚。如果 IT 部门不能达成以上目标，则其组织可能面临经营风险，对社会形成危害甚至受到刑事制裁。

在承担以上职责时，IT 经理人不能再一而再，再而三地购买新的产品来应付层出不穷的不断占据着技术及商业媒体头条的各种需求。商业价值，安全和法规遵从等各个层面的需求要求企业能够实现统一的响应。CIO 们需要的是可以帮助他们淘汰不再需要的技术和过程并可在一个通用的工作流中整合多种具备完全不同要素的解决方案。虽然现有的企业软件厂商已经开始采用整合的设计和开发方式，但由于商业和技术方面的原因，他们的产品线不得不与传统绑定在一起。执行彻底的改变会影响其用户既定的收入流，更不用说改造或替换废弃的产品在技术上会给用户带来的巨大风险。

正因为现有的厂商无法放弃已经过时的技术，所以 IT 组织应从现在开始着手寻找新一代的基础架构管理平台，其中尤为重要的是需要将平台与工具集区分开来。一个管理平台可以为实现基础架构管理服务提供表述、交付，报告和评估的基础和通道。从各方面来看，其最重要的功能在于为管理服务的交付打造一个统一的，长期可用的坚实平台，通过平台提供的工具和服务可在其各自的生命周期中往复使用。一个稳定坚固的平台能够让 IT 人员在提供服务的过程中更为专注并可以不断提供日益深化的服务。与之相对应的是，工具集则可能包括大量单一功能的修复工具，每一种工具都有其各自的接口、界面，方法论和工作方式。而每一种工具的相关管理工作都会与交付管理基础架构自身所需要的硬件，软件和操作手册等工作一样多，因此经常会把 IT 人员搞得顾此失彼，严重影响工作效率，无法真正提高 IT 管理水平。

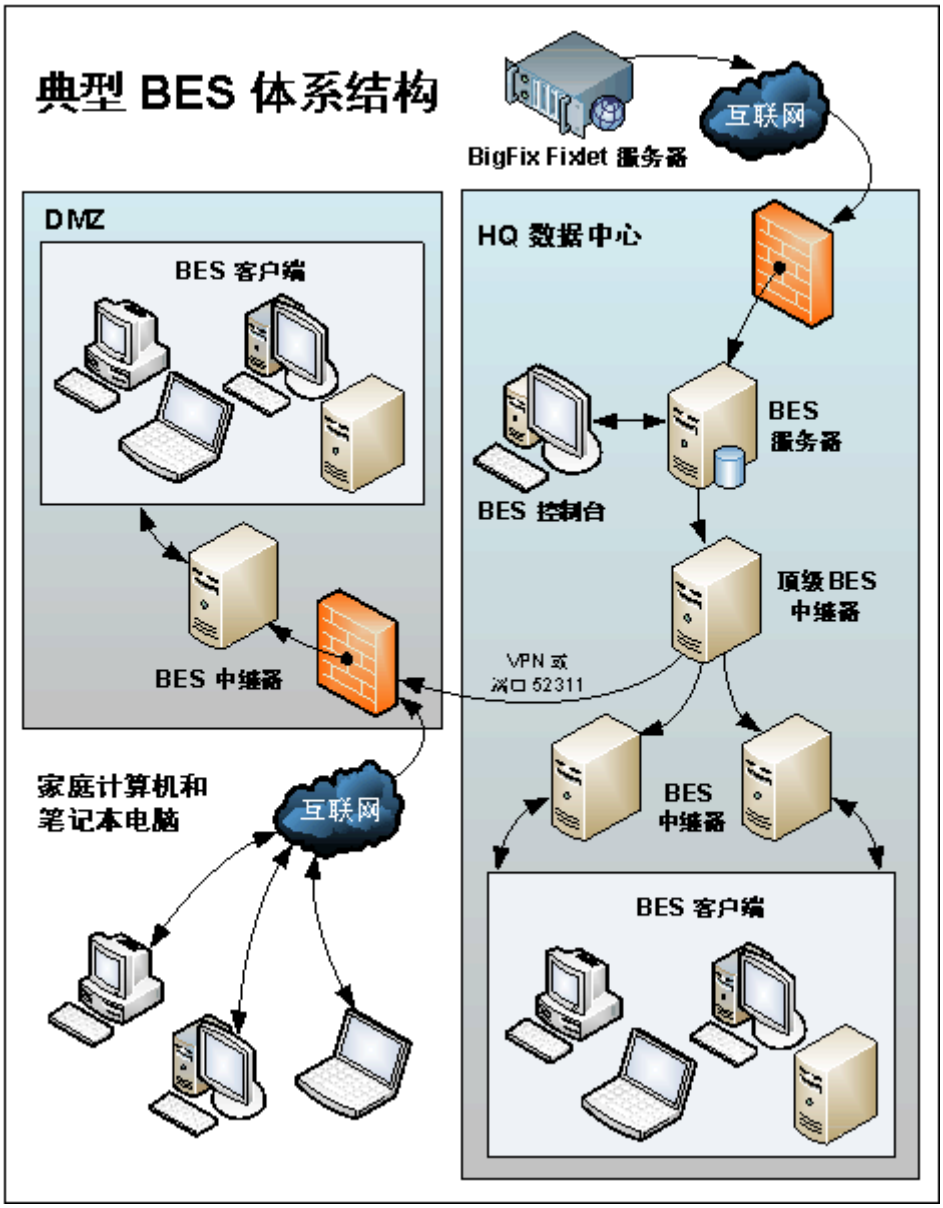
3 BigFix 平台

BigFix 解决方案的设计目标不是去应付一个预先设定好的环境，而是要在未知的环境中可以游刃有余地工作。BigFix 一直在致力于打造一个统一的通用问题处理平台而不仅仅是解决当前所遇到的问题。无论面临的问题是什么，该平台都可以为问题的解决提供基础架构和方法论。

BigFix 解决方案的核心是一个具备大规模可扩展能力的分布式处理系统，可通过单一的策略驱动代理实时不间断地发现、评估，修复和强制分布式企业中所有台式机，移动终端和服务器的健康和安全。BigFix 的专利技术可以将计算能力分配给企业中轻量级、多功能的智

能 BigFix 代理，提供传统解决方案所不具备的可见性和控制能力。BigFix 是一种可以从根本上改变 IT 运作方式的革命性技术，在及时性、灵活性及可扩展性等方面具备极大的优势，同时可以大幅减少传统的系统及安全管理架构所需的基础架构及培训成本。

3.1 分布式可视及管理神经系统



BigFix产品由BigFix核心服务平台和面向问题的策略库组成。BigFix核心服务——包括BigFix代理、BigFix服务器、BigFix控制台，BigFix中继器和Fixlet消息——构成了一个轻量级的、动态的内容驱动型消息和管理控制系统。此系统可以由基础架构管理人员执行策略设

置，将管理IT基础架构的工作分配到被管理设备自身完成。

这种方式与传统的依赖于中央服务器实现所有信息处理的客户端/服务器管理系统模式不同。传统的系统虽然也可以利用代理技术，但是其代理对于中央管理资源来说往往处于次要地位。要执行一个典型的管理动作，这些解决方案需要执行一系列的资产清单和查询动作，然后还需要等待代理的响应。这会对网络和服务器带来极大的负担，更不要说必须强制对这些信息进行刷新的操作员。基本上来说，传统的系统管理工具就像是一个拥有许多触角的大脑，如果触角不能连接到大脑则会完全失去作用。更糟的是，管理动作对于当时不能连接到网络或中央服务器的设备完全不可达，且这些设备对于基础架构管理人员来说完全不可见。

BigFix 代理则位于被管理的终端上，不管当前是否终端可以连接到 BigFix 服务器，BigFix 代理都会不断用组织指定的用于驱动 IT 执行的问题对终端进行检查。BigFix 同样拥有一个具备众多触角的中央神经系统，这些触角可延伸到组织网络的各个角落，不同的是这些触角具备本地的智能。这意味着 BigFix 可以在任何地点，任何时间工作，而不必在意某台被 BigFix 管理的资产是否可与组织网络连接。

3.2 BigFix 代理

每台BigFix可管理的台式机，笔记本和服务器都需要运行BigFix代理，代理可不间断地执行由BigFix服务器发出的策略指令（Fixlet消息）。一个单一的BigFix代理可以执行多种策略，而不需要部署多个代理来实现多种单一的功能。这种方式可以减少多种工具间的混乱，管理上带来的麻烦和软件许可证费用。此外，管理动作和结果还可实时上报给BigFix控制台。

BigFix的终端智能对于实现无组织信息的收集和异常问题的查询尤为重要。当需要查询新的关于终端配置状态的问题时，管理员可以编写自定义的Fixlet消息或从已有的BigFix策略库中发送预打包的Fixlet消息给每台网络中的BigFix代理。这种Fixlet消息包括问题的定义和用于确定终端是否存在此问题的计算机可识别的属性清单。当代理响应Fixlet消息时，会根据属性清单分析其本机状态以决定是否本机受此问题的影响。如果终端存在此问题，代理会向BigFix服务器发送简短的报告。对于存在的问题，代理可向服务器请求修复内容在终端上执行，安装相应的修补程序并报告问题处理结果。

这种可实时决定哪里存在问题的技术具备三种主要的优点：首先，将实现管理的计算负载分布到整个环境中，使得评估和修复过程可并行完成，每个BigFix代理仅需花费几秒钟的时间用于检查其自身状态，以决定其是否满足某些特定的条件。而其它系统管理工具则需要扫描整个基础架构，将数据传输到服务器，再由服务器筛选这些数据以决定是否有计算机符合特定的条件，从而确定有问题的数据。整个过程可能需要花费数小时，数天甚至数周的时间。

第二，因为驻留在终端的BigFix代理可以持续评估本机状态并报告相应的结果，所以服务器不需要对所有代理运行查询来决定是否某计算机资产有问题。每个终端可即时响应并提交查询结果。

第三，传统系统管理工具要实现扫描和修复过程需要传输和保存大量数据。由于BigFix代理软件可本地检查其终端属性，因此BigFix不需要投入专用的网络和服务器资源来应付传统工具所需要处理的海量数据。再有，传统系统管理工具需要传输所有的数据以实现服务器端的分析，而BigFix代理只有在其所驻留的终端存在问题时才会报告。

总而言之，BigFix 可以提供企业 IT 环境中所存在问题的实时视图，而不必等待可能数周前就已经存在的问题的滞后报告。这种实时可见性和控制能力可以大幅减少网络基础架构，服务器和资产自身的负载，并可通过减少查询/修复动作的模糊性和不确定性来提高 IT 组织的操作效率。

BigFix 代理支持操作系统平台如下：

- **Windows**
  - Windows NT SP6a/95/98/Me/2000/XP/2003 with IE 4.01+ (x86)
  - Windows 2003/XP (x64)(including Windows 2003 R2)
  - Windows Vista (x86/x64)
  - Windows 2003 Itanium
  - Windows Server 2008 (x86/x64)
- **非 Windows**
  - HPUX 11.00/11.11/11.23 (RISC)
  - HPUX 11.23 (Itanium)

- IBM AIX 5.1/5.2/5.3 (PowerPC)
- Solaris 7/8/9/10 (SPARC)
- Solaris 10 (x86)
- Linux Red Hat 8/9 (x86)
- Linux Red Hat Enterprise 3/4/5 (x86/ x64)
- VMWare ESX Server 3
- Linux Red Hat Fedora Core 3/4/5 (x86)
- Linux SUSE 8/9/10 (x86)
- Linux SUSE 9 (x64)
- Mac OS X 10.3/10.4/10.5 (PowerPC)
- Mac OS X 10.3/10.4/10.5 (Intel)

3.3 BigFix 服务器和控制台

BigFix 服务器作为 BigFix 解决方案的可视和操作中心，可安装并运行在低成本的 Windows 平台计算机上。BigFix 服务器是管理数据，向 BigFix 代理发送策略并从代理接收数据的核心，同时以 BigFix 控制台的形式提供管理用户界面。一台普通的运行 BigFix 服务器的 x86 计算机可以管理超过 50,000 台安装 BigFix 代理的设备。此外，BigFix 服务器软件还可实现分权控制，即可以按照需要（根据组织结构或其它因素）将管理权限分配给相应的管理员。

BigFix 服务器配置及可管理的客户端数量如下：

部署规模	CPU	内存	硬盘
< 250	2-3 GHz	1 GB	Standard HD
1,000	2-3 GHz - 2 Cores	2 GB	1 RAID Array (RAID 10, 5)
10,000	2-3 GHz - 2-4 Cores	4 GB	1-2 RAID Arrays (RAID 10)
50,000	2-3 GHz - 4 Cores	8 GB	2 RAID Arrays (RAID 10)
100,000	2-3 GHz - 4-8 Cores	12 GB	3 RAID Arrays (RAID 10)
> 200,000	2-3+ GHz - 8-16 Cores	16+ GB	3-4 RAID Arrays (RAID 10)

3.4 BigFix Fixlet 消息

BigFix Fixlet 消息向 BigFix 代理传达策略信息和指令。Fixlet 消息包含确定动作对设备可执行时需要设备所满足的逻辑条件（例如，设备需要符合某一特殊条件），可编程的指令（“如果此客户端存在漏洞 X，升级软件模块 Y”），配置参数（如调整个人防火墙阻断所有进入端口 445 的通信）和可以执行的内容（进行安装的软件升级包）。Fixlet 消息可由 BigFix 或第三方作为预置的，即时可用的策略内容提供给用户，或由用户自己使用 BigFix Fixlet 消息关联语言编写。

BigFix Fixlet 关联语言是一种可发布的命令语言，可以让 BigFix 用户，合作伙伴和开发者为使用 BigFix 所管理的资产创建自定义策略和服务。该语言可被用于解决每个大型企业经常会遇到的问题，如补丁部署、配置管理，反病毒管理及软件分发等，或者被用于编写快速的查询及补救措施以便解决每个企业 IT 运营维护人员几乎每天都会遇到的各种繁杂的问题。尽管 Fixlet 关联语言是 BigFix 向其客户分发策略内容的主要方式，但它并不是私有的。BigFix 提供关于关联语言的培训课程并鼓励 BigFix 的客户和第三方合作伙伴使用其作为安全和系统管理的通用语言。

3.5 BigFix 中继器

BigFix 核心服务还包括一种可在分布式环境中保证高效通讯的重要机制——BigFix 中继器。在实现 BigFix 解决方案时，管理员可指派几乎任何被 BigFix 代理所管理的计算机作为 BigFix 中继器。BigFix 中继器可通过对数据的压缩和分配及为 BigFix 的策略、修复内容和代理通信提供容错通讯点来减少支持 BigFix 服务所需的带宽。BigFix 中继器不需要专用的计算机，且可在 Microsoft Windows 环境中作为共享服务运行，终端用户可以使用安装了 BigFix 中继器的计算机工作，而不会注意到性能的下降或处理器/内存超负荷。事实上，许多终端用户完全不在意他们的 IT 资产是否还在企业中提供中继服务。

为了提高对于移动及远程设备的管理，BigFix 代理可以支持中继自动选择。这能使所有 BigFix 可管理的资产无论其位置都可以发现已注册的中继器。这种机制提供了极为强大的自适应能力，因为移动的设备即使不能连接到公司的网络或不通过 VPN 连接也可以自动与最

近的，可靠的 BigFix 中继器通信。

4 BigFix 解决方案

BigFix为在企业基础架构中交付全面的安全和系统管理服务提供了强大灵活的平台。借助于BigFix核心服务平台，使得BigFix开发和提供不断完善的组合式服务成为可能。

BigFix 解决方案集将涉及高优先级企业 IT 问题的策略内容模块组合在一起。当前，BigFix 解决方案集包括：系统生命周期管理——自动化并简化常用的系统管理任务；安全配置和漏洞管理——处理针对企业完整性的过程和人为风险；BigFix 终端防护——采用集成的方式防御安全威胁。借助于 BigFix 核心服务平台作为承载工具，所有的 BigFix 解决方案集使用共有的，统一的管理方法实现各自的功能。这不仅可以使以前各种独立的服务的交付得到整合和标准化，还可以帮助全体员工加深对于这种管理方法的理解和熟悉程度，从而提高生产力并减少出错的风险。

4.1 BigFix 系统生命周期管理

BigFix 系统生命周期管理解决方案集将 BigFix 的经济学和卓越的运作纳入到关键的 IT 运营管理功能中，如资产发现/管理，电源管理，软件分发，补丁管理和远程协助等。通过整合和简化最常用的 IT 操作过程，BigFix 可以实现兼具细粒度准确性的最高级的自动化，使 IT 部门可保证其服务水平，致力于战略性的工作并保证总体的运营效率。

4.1.1资产/License 管理

BigFix 资产/License 管理模块可以轻松地跨越多个地理位置及分布式网络，实现企业计算机网络的统一管理和资产收集。BigFix 资产/License 管理能够帮助企业了解当前所有被管理计算机的资产信息，弥补固定资产报表的不足，并能为软硬件升级计划及充分提高现有设备的利用率提供极为有益的基础信息。

此外，该模块还可以发现网络中有哪些设备并主动进行维护以使其遵从配置标准和基线。

BigFix 资产/License 管理模块可实现所有 LAN 和 WAN 连接设备的可见，而不论其是否被授权，是否可被 BigFix 管理。独有的基于代理的分布式扫描技术可以在本地检测 BigFix 不可管理的设备，并使用最小的延迟和网络带宽需要将结果回报给 BigFix 控制台。此模块具备以下特点：

- 可快速，完整地识别未登记和游离的设备（使用 IP 的设备），而不管这些设备上是否安装了 BigFix 代理
- 报告未管理资产使用的端口及服务
- 通过部署 BigFix 代理将未管理资产纳入到企业统一管理体系中
- 独有的分布式扫描基础架构可实现低影响，低延迟的未管理设备检测和报告
- 及时交付新加入或已存在于网络中的资产的信息，支持特别查询及上报
- 提供准确，实时的 IT 资产详细清单，为系统的软硬件优化创造前提条件
- 识别已安装软件和许可证的详细信息，持续监控和跟踪应用程序的使用
- 可添加自定义的资产属性，以提高企业对设备管理的有效性及关联性
- 支持静态和动态的资产分组管理
- 保证遵从组织标准及策略
- 大幅减少由于错误配置产生的故障停机时间和安全间隙
- 高可扩展能力，对网络操作及被管理设备性能影响最小

4.1.2软件分发

BigFix 的软件分发功能可以完美地解决动态的网络环境中繁杂的应用软件及文件的部署和分发任务，使软件分发过程实现自动化，提高一次性通过成功率，增加新的保障级并实现对软件分发和部署过程的验证。通过 BigFix 可以使终端用户始终保持升级到最新发布的程序和服务包，提高 IT 人员和终端用户的生产力。此模块具备以下特点：

- 在大型分布式环境中安装或升级软件，自动删除废弃的或未授权的软件
- 自动化的软件安装闭环验证，实时反馈软件分发状态信息
- 利用 BigFix 中继器网络可本地预缓存软件包以节省网络带宽并提高安装可靠性
- 利用 BigFix 代理+中继器的架构可节省网络带宽及计算机处理资源

- 全面的软件交付控制
  - 断点续传，分时处理，多通道机制，静态/动态带宽管理
  - 可让高优先级的任务或网络流量先行
- 支持 Windows、UNIX，Linux 和 Macintosh OS X
- 与正在使用的软件分发工具兼容并互补
- 缩短时间周期，大幅提高可验证的软件分发一次性通过成功率

4.1.3补丁管理

对于大量的大中型企业来说补丁管理一直是最棘手的问题。组织要将安全与系统管理过程置于掌控中其首先需要解决的问题就是实现高效的补丁管理。BigFix 的补丁管理模块可缩短补丁和升级的部署时间，减轻工作量，消减费用并提高操作系统和应用程序补丁处理的效率。借助于 BigFix 的统一管理平台，用户可实时修补系统安全隐患并将补丁程序由 BigFix 服务器发送到成千上万台计算机，同时确保整个过程的可管理性和可控性。此模块具备以下特点：

- 为 Windows、Linux，UNIX 和 Macintosh OS X 提供实时的补丁评估及修复
- 为 Windows 及第三方应用程序提供补丁管理
- 终端自我评估并通告需要的补丁及升级——无需集中式扫描
- 已损坏补丁的检测和修复，可实现最小的补丁间隙和最大的范围覆盖
- 支持高效的，带宽敏感环境下的补丁内容分发
- 向导和脚本工具可为几乎任何软件分发和安装补丁，无论是购买的还是自己开发的软件
- 补丁修复状态闭环验证
- 支持补丁的回退
- 遵循 BigFix 的补丁管理实践可使首次通过成功率由使用 BigFix 解决方案之前的 60-75%提高到 95-99%甚至更高
- 在主流 IT 业界及媒体的独立产品评测中屡次被评为最佳补丁管理产品

4.1.4电源管理

以企业规模应用桌面系统的节电方案可大幅减少电费的支出及造成温室效应的碳排放量，实现节能减排的目标。BigFix 电源管理模块可使企业用户轻松应对企业计算机电源管理的复杂性，真正应用计算机节电技术。此外，BigFix 电源管理模块还集成了 BigFix 独有的分布式网络唤醒技术，以使电源管理与终端用户的工作周期及系统管理维护时间窗之间实现真正意义上的同步。此模块具备以下特点：

- 集中化的，策略驱动型分布式计算机电源管理，范围可从一台单独的计算机扩展到整个全球化的企业网络
- 对系统待机/休眠，子系统（硬盘/显示器等）的停用实现精确的控制
- 可对设置实现分组控制，为不同的计算机组设置不同的电源管理方案
- 独有的分布式计算机网络唤醒（Wake-On-LAN）技术，使系统维护过程与节电管理同步
  - 避免了许多网络不能在不同子网间路由网络唤醒数据包的问题
  - 可通过 BigFix 客户端唤醒同子网的其它计算机
  - 快速制定网络唤醒计划
- 控制 Windows 和 Mac 系统的电源设置漂移
- 图形化的用户界面，展示板驱动型的策略设置及报表
  - 可以让企业测量可能节约的电量
  - 给出关于执行情况的简单报告
  - 可查看指定时间段内的节电设置，能源使用和费用情况

4.1.5远程协助

微软从 Windows 2000 开始在操作系统中加入远程桌面功能。微软的远程桌面功能（远程桌面和远程协助）是被许多组织广泛应用的全功能产品，但是由于缺乏企业环境下的管理能力，导致企业通常不能充分发挥其效用。

BigFix 远程协助模块可以简单地让企业充分利用 Windows 的内建组件来实现全功能，

符合最高安全标准的企业级远程桌面管理。企业使用 BigFix 远程协助模块可为 Windows 远程桌面带来设置和许可的集中可见性和可控性，并可通过 BigFix 控制台的简单操作对企业级规模或部分计算机进行配置。此模块具备以下特点：

- 结合 BigFix 的实时系统管理和 Microsoft 远程桌面及协助工具
- 为帮助台提供 BigFix 所具备的实时可视及控制能力
- 可使用 BigFix 的分权管理特点定义帮助台操作员的角色和职能
- 访问 BigFix 修复过程（补丁，软件升级和策略管理等）以远程解决终端用户的问题
- 提高帮助台交互的质量及效率

BigFix 还可为用户提供第三方集成的远程控制功能。用户可随时将远程控制的服务端软件分发到终端并进行远程协助，在完成支持任务后，可卸载远程控制的服务端以确保客户端的数据安全及隐私保护。集成的第三方远程控制工具具备以下特点：

- 能够实现管理员对远程桌面电脑的操作和管理
- 支持客户端授权模式，只有经过终端用户许可，管理员才能对其进行远程操作和协助
- 进行远程操作和协助时，可根据管理员需要进行全屏操作或锁定被管理计算机的键盘、鼠标
- 可实现远程计算机的锁屏、重启与关机
- 可实现管理端和远程计算机之间的文件复制及文字对话功能

4.2 BigFix 安全配置和漏洞管理

BigFix 安全配置和漏洞管理模块解决方案集中包括安全补丁管理、漏洞管理，网络游离资产发现和基于最佳实践与技术控制的安全配置管理等解决方案。该方案集可以节省费用、减少复杂性，降低安全风险，并可将信息安全管理工程由被动的，救火队员式的危机处理转化为早期的，主动的风险管理。

4.2.1安全配置管理

当前，需要被保护的企业其计算能力及计算机环境的参与者正在呈指数级增长，所以安全配置管理需求对于企业来说也变得愈发的重要。由于业界最佳实践，政府机构要求和行业规范的参与，实现高效安全管理的解决方案也不断趋于标准化。美国国防信息系统局（DISA），国家标准与技术研究所（NIST），国土安全部（DHS）和国防部（DoD）等机构开发了一系列针对不同操作系统平台的配置标准，要求美国各联邦机构和军队机构必须遵从，以提高信息安全并减少整体 IT 运营费用。同时，许多私营企业也采用这些政府标准作为内部规范。BigFix 可以在整个组织中为制定和执行这些策略规范带来前所未有的实时可视及控制能力。

BigFix 安全配置管理模块提供全面的技术控制集，可在 Windows，UNIX 和 Linux 系统上检测和执行组织的安全配置策略，帮助 IT 组织达成法规遵从和最佳实践的目标。此模块具备以下特点：

- 实现自动化的配置可见，设定及强制
- 通过订阅来自 BigFix 的，可即时应用的修复策略使安全配置管理遵从来自 SANS 学会，美国国家标准技术研究院（US National Institute of Standards and Technology（NIST)），美国国家安全局（US National Security Agency（NSA））和微软的最佳实践
- 可选择支持美国国防信息系统局技术规范（Defense Information Systems Agency Security Technical Group（DISA STIG））和美国联邦桌面通用配置（Federal Desktop Common Configuration（FDCC））标准的 BigFix Fixlet 消息库，每个策略控件映射相应的标准参考 ID
- 包括BigFix安全策略管理器，可通过订阅不断丰富的，预打包的Fixlet消息库来实现安全配置策略遵从并使策略配置自动化；可覆盖多方面的安全配置，包括MS Office/IE/Outlook安全配置检查、网络连接管理、外设管理、网络共享管理、进程及服务管理，屏幕保护设置和密码策略等等
- 整合多种策略驱动型配置管理模版，降低安全审计费用及安全风险

- 可对离线的终端进行策略强制
- 特别查询及上报
- 客户端自我监管，可不间断根据配置基线进行评估及修复
- 可自定义内容满足多样化的安全配置管理需求
- 将修复周期由数天或数周缩短为数分钟或数小时
- 在弱点和漏洞被利用前主动进行封堵
- 实时的报告满足目标和法规遵从需要

4.2.2漏洞评估

BigFix 漏洞评估模块可依据来源于 MITRE 公司脆弱性评估语言 OVAL（Open Vulnerability Assessment Language）的漏洞评估定义知识库对所有安装了 BigFix 客户端的终端进行主动的系统安全漏洞评估，以实现对企业网络脆弱性检测的基准测试。此模块具备以下特点：

- 主动的风险评估和风险管理
- 不间断评估系统状态，识别安全漏洞但不影响系统性能
- 对可识别的漏洞进行安全等级和优先级划分
- 对连接企业网的固定终端和离线的移动计算机进行全面的漏洞管理
- 兼容 MITRE OVAL/OVAL-ID

4.3 BigFix 终端防护

BigFix 终端防护方案集将多种最重要的终端防护服务结合在一起——包括防病毒、反间谍软件，网络准入控制和终端防火墙等——管理员可以通过 BigFix 统一管理平台对这些服务进行无缝的集成管理。借助于单一的代理和单一的管理控制台，BigFix 终端防护方案集可消除由于使用多种安全工具所带来的复杂性，混乱性及高昂的费用，可在全球规模实现主动的，先发制人的策略驱动式终端防护而无须增加管理和使用成本。更重要的是，IT 人员可通过他们在实现系统生命周期管理和安全配置及漏洞管理时使用的同一 BigFix 基础架构和管理控制台来实现终端防护。

4.3.1防病毒

无论终端是否连接到企业网络，BigFix防病毒扩展模块都可以维护被管理的终端免受计算机病毒的侵害。该模块可以部署特别针对BigFix进行优化的防病毒客户端到联网的终端，不间断地对系统进行监控，执行按需及定时病毒扫描，更新病毒定义文件，评估网络健康程度并通过展示板跟踪工作进度。此模块具备以下特点：

- 突发威胁快速响应——利用快速响应中心网络实现对病毒威胁24 x 7的监控和响应
- 多种检测技术——包括特征匹配及高级启发式检测
- 强制防病毒策略——BigFix终端代理可确保防病毒软件客户端的安装和运行，弥补一般防病毒软件5-15%的部署间隙
- 跨平台的集中报表——可为多平台环境及分布式网络提供全面、准确，统一的防病毒状态实时报告
- 自动当日下载最新的病毒定义文件及更新，将Windows漏洞暴露时间窗减至最小
- 闭环反馈信息——从每台终端接收实时状态，能使IT人员在几分钟内确认升级文件的成功交付而不会对网络带来影响
- 最低的误报率，最广泛的覆盖，确保高水平的方案完整性

4.3.2终端防火墙

BigFix终端防火墙扩展模块通过BigFix控制台对终端防火墙的管理进行集成和强化。该模块可结合并对应BigFix的策略来实现基于终端状态细粒度评估的网络访问级别定义，动态并自动地根据环境标准调整防火墙策略。此模块具备以下特点：

- 采用独特的评估，修复及连接（ARC）工作模型，允许管理员根据终端安全状态动态定义防火墙的访问控制策略
- 强大的包检测及过滤技术
- 提供细粒度的策略强制
- 具备位置感知技术，可在任何时刻检测终端访问企业网络的连接类型——LAN，VPN还是WLAN，当连接类型变化时可自动调整访问控制策略

- 应用级阻断可为出入终端的通讯提供特殊的控制
- 集成网络准入控制功能，可实现终端基于安全策略的自我隔离
- 通过控制台实现实时的可视及可控

4.3.3反间谍软件

间谍软件和其他恶意软件会威胁到组织业务的连续性，需要花费一定的时间进行修复，从而降低员工的生产力并威胁到敏感的组织和客户数据。目前在互联网上已有数万种程序可窃取数据或可让攻击者访问目标计算机。跟据微软公司的统计：不需要的，恶意的程序导致了 50%的 PC 崩溃事件。

BigFix 反间谍软件扩展模块以可扩展的，实时可控的 BigFix 平台为基础，可帮助 IT 部门减少用于修复被破坏的 IT 资产的费用，并保护计算机及敏感信息不受间谍软件和其他有害软件的威胁。此模块具备以下特点：

- 提供针对间谍软件、广告软件、击键记录软件，远程访问木马程序及浏览器劫持工具的全面保护
- 采用独立的专用反间谍软件引擎，兼具特征匹配及高级启发式检测技术
- 采取主动保护，可清除内存中运行的有害程序，在间谍软件窃取敏感信息前及时予以清除
- 可对反间谍软件进行快速高效的升级
- 提供有害软件感染情况，清除状况及危害程度的集中报告和分析
- 将由间谍软件威胁带来的漏洞暴露时间窗减至最小

4.3.4第三方防病毒软件客户端管理

通过 BigFix 的实时可见及可控的基础架构可强化并简化第三方防病毒软件客户端的管理。该模块不仅可以将防恶意软件的防线置于 BigFix 的管理架构之下，还可以为专有的恶意软件防护管理架构带来前所未有的扩展能力，速度及完全性，使组织能够真正走在外部威胁的前面。此模块具备以下特点：

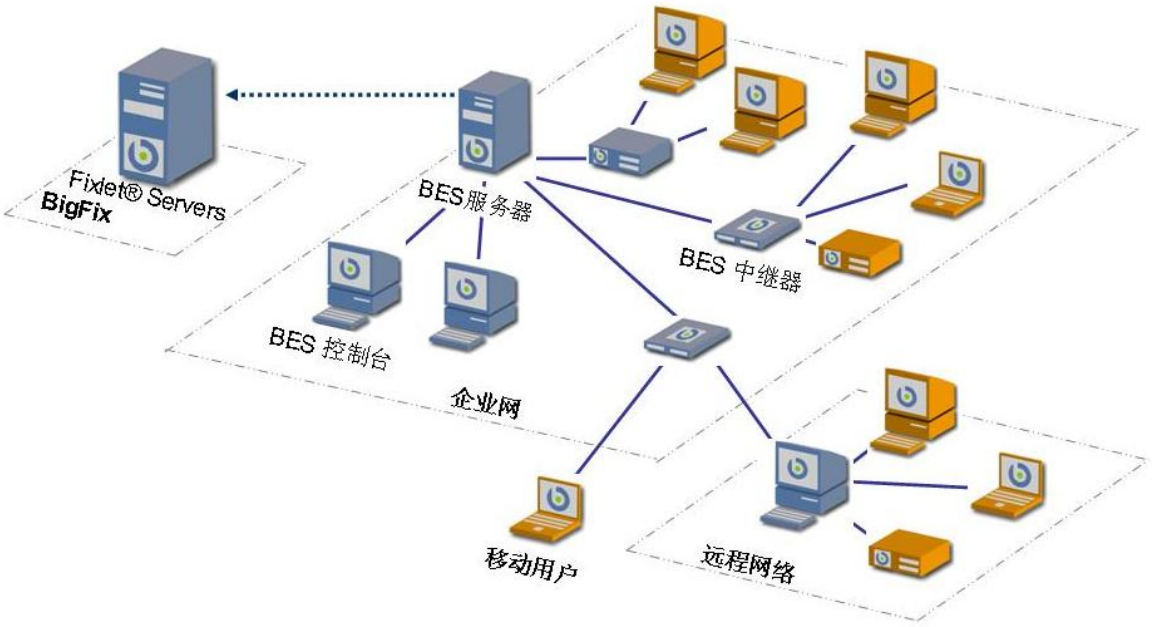
- 为防病毒和其他安全及系统管理服务提供单一及可升级的管理点；实现统一的管理视角和控制
- 实时展现当前使用的防病毒软件客户端和恶意软件特征识别状态
- 在多品牌环境中实现快速，可靠的 DAT 升级文件分发
- 支持 CA eTrust，Kaspersky，McAfee VirusScan，Rising，Symantec/Norton，Sophos 和 Trend Micro 等防病毒产品
- 弥补 Windows 计算机使用环境中 5-15%的防病毒软件覆盖盲点
- 降低防病毒软件管理成本并提高其管理质量

4.3.5网络准入控制

BigFix 网络准入控制模块可根据网络准入策略实现终端的自我评估和强制。此外，还可扩展第三方网络准入控制（NAC）解决方案（Cisco，Infoblox，Microsoft，H3C 和 Symantec 等）的功能，为其提供单点的安全状态评估和修复。此模块具备以下特点：

- 可实现单点安全状态评估和修复，简化管理并减少混乱和冲突
- 基于策略的终端安全状态评估，自动修复被隔离的设备，快速召回被隔离的计算机
- 提高第三方 NAC 解决方案的性能并弥补其功能的缺陷
- 终端自我调节：可以不间断地对终端合规性进行自我评估及修复——通过“预调解”避免不必要的隔离
- 可根据终端环境（已连接，无线，远程/Internet，VPN 等）改变策略，以实现灵活及强大的访问控制
- 使用 Windows 自带的 IPSec 策略实现基于终端安全状态的网络准入控制
- 灵活的评估策略，确保组织安全配置策略的继承和强制

5 部署与使用



如上图所示，在企业网络中部署一台 BigFix 服务器，定时与位于互联网的 BigFix Fixlet 服务器通信，下载最新的 Fixlet 策略消息。

在网络中所有的服务器，台式机和笔记本上安装 BigFix 客户端程序，由 BigFix 服务器统一管理。

BigFix 中继器可通过控制台实现远程安装、启用和管理。BigFix 系统使用中继器汇聚并转发所有 BigFix 系统的文件传输和通讯。可在企业网中的适当位置如每个网段内部署一台中继器。当一个补丁需要分发到一组计算机，这个补丁可以由 BigFix 服务器直接分发到目标系统或者由服务器传送到中继器，然后再由中继器分发到本地局域网的目标系统。这种分级的结构大大减少了 BigFix 服务器的工作压力。BigFix 中继器可实现多级级联，每台中继器可对所有上下行的通信进行中继，无须客户端与 BigFix 直接对话。每个 BigFix 客户端可以自动发现、使用距自己最近的 BigFix 中继器，最大程度减少人工部署和干预。

对于远程的办公地点，BigFix 中继器可以部署在远程的办公地点现有的服务器或工作站上，作为文件的缓存及本地数据分发的转发中继。采用这种方式可以节省广域网络带宽，将

BigFix 客户端和中继器/服务器间的通信量降低到最小程度。

6 BigFix 产品特点及优势

6.1 实时可见及可控

借助于灵活的，获得专利的检测引擎架构，BigFix 几乎可以从远程计算机上获取任何信息，并发送到中央服务器进行分析和报告。关于文件系统（大小、文件类型、版本、修改日期，hash 校验值和位置等）、WMI、DMI、硬件、安装/运行的软件、安装/运行的服务，BIOS 和操作系统等的任何数据都可被检查以实现属性的获取。被获取的属性集可由管理员完全控制以限制收集感兴趣的资产信息所需要的传输带宽。这种机制为管理员提供了鉴别资产的极为强大的工具。管理员可在网络中确定问题的范围（如问题存在于关键的/非关键的资产上）并决定在哪里应用解决方案。

BigFix 的架构可以允许几乎实时地对网络中的问题及资产进行分析。BigFix 系统的漏洞检测与修复机制可为管理员提供几分钟以前的信息，几乎实时地跟踪那些受某问题影响的计算机及为修复这些计算机而执行的动作是否成功。

6.2 整合与控制

单一功能解决方案的大量使用在以指数级增加着企业安全操作的复杂性，因为每个单点的产品都需要专门的管理及多余的硬件基础架构。BigFix 的统一管理平台可以以几乎 40:1 的比率整合服务器，为所有的台式机，笔记本电脑，服务器提供轻量级的实时控制能力，而不用在意其操作系统或位置。

6.3 单一可信来源

因为 BigFix 的架构具备轻量级及高可扩展性的特性，组织在其已有的软件管理解决方案之外还可以部署 BigFix，用 BigFix 来即时查看其他软件工具的工作情况，发现它们有什么不足并实时确认已执行的动作。BigFix 提供大量的报表和展示板，还可与第三方配置管理

数据库相结合以作为单一的可信来源。

6.4 卓越的可扩展能力

BigFix 平台具备卓越的可扩展能力，适应大规模分布式网络部署，单独的中央服务器可支持 200,000 台以上计算机系统的管理。BigFix 先进的中继技术可实现多级中继的自动级联部署，并具备对所有上下行通信的中继能力，无需客户端与中央服务器直接通信，尤其适用于大型分布式网络架构。BigFix 还提供基于每个终端，每种连接类型的智能化的带宽管理能力以实现对网络影响的最小化。BigFix 系统使用标准的 HTTP 协议，可跨网段部署，IP 可达即可工作。即使网络中部署多种类型的防火墙和访问控制工具或使用 NAT 也可以实现实时的全网终端统一管理。

6.5 最小客户端资源占用

借助于 Fixlet 的智能处理能力，BigFix 可以实现独有的单代理多功能技术，即客户端只需部署一个客户端代理程序，开启一个服务即可完成众多的管理任务，可大大降低客户端部署及工作复杂性，稳定性高。

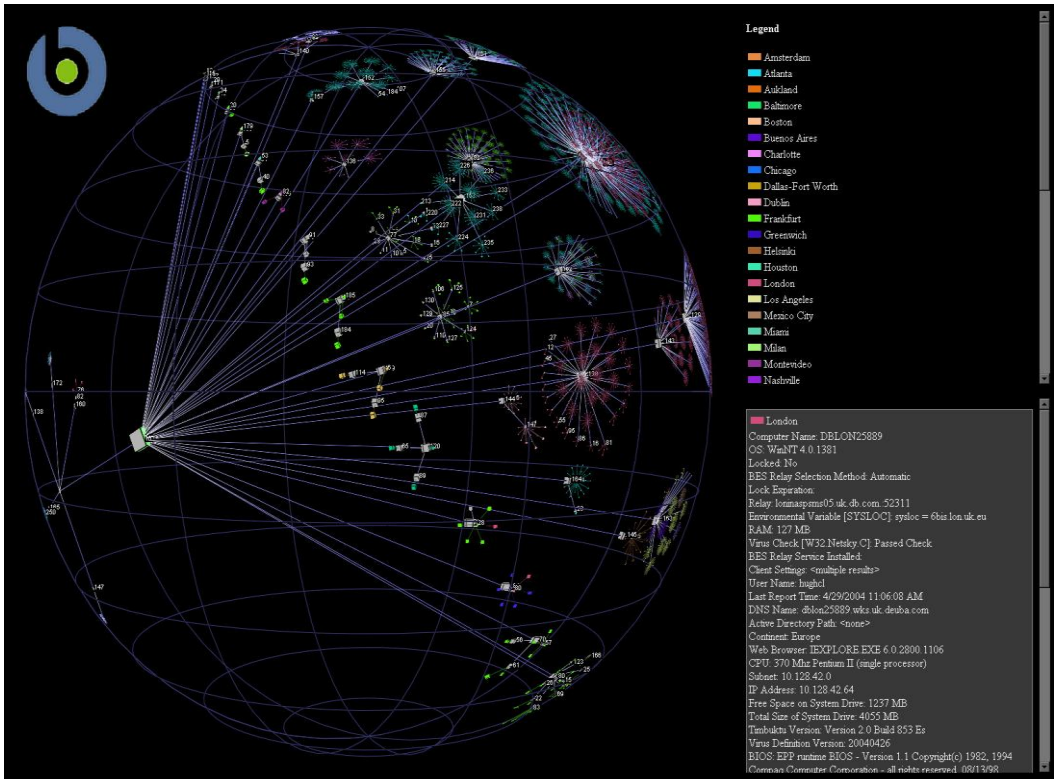
同时，客户端对本地资源的占用也是企业用户最关心的问题。BigFix 采用先进的 CPU 时间片管理机制，可由管理员根据系统角色及使用环境确定客户端检测引擎占用的 CPU 资源，缺省不超过 2%。如此，既可以保证 BigFix 客户端在第一时间发现系统安全隐患进行修复，又不会影响终端系统正常使用。

6.6 可靠的系统安全性

BigFix 系统采用基于证书机制的双因子认证技术，而不仅仅依赖操作系统自身的安全性。采用这种方式可以最大限度地保证终端系统的安全，即使 BigFix 服务器完全被攻击者控制，但只要管理员的私钥文件或私钥密码没有泄露则攻击者依然无法利用 BigFix 平台对终端进行任何违规的操作。

6.7 可视化管理

BigFix 不但提供直观，简洁的管理控制台界面，而且还提供三维的图形化管理界面，便于管理员直观地了解所管理计算机的整体状况。



6.8 全面的解决方案

BigFix 的功能以模块形式提供，这种模块化的功能基于 BigFix 的 Fixlet 专利技术，当您想添加新的功能时，只需要订阅新的“内容”——Fixlet 消息就可以了，无须重新安装和培训，不用添加额外的硬件，不用编写新的脚本，新的功能可立即启用。BigFix 通过平台可提供多样化的解决方案。

6.9 强大的定制能力

BigFix 借助于强大的 Fixlet 技术可以为用户提供多样化的产品模块和服务。组成各个产品模块的 Fixlet 消息经由 BigFix 公司预打包和测试后分发给用户，可大大节省用户部署和

应用各种解决方案的时间。同时 BigFix 还提供强大的自定义和向导功能，用户可以自己编写 Fixlet 或通过 BigFix 的专业服务团队来实现特殊定制的功能，完成异常问题的检测，修复和汇报，解决各种终端安全配置管理问题，满足多样化的需求。

6.10 先进的离线管理能力

BigFix 采用先进的分布式处理模型，一旦服务器将策略分发到客户端，客户端的检测引擎就可以自主运行，对 Fixlet 的相关性进行检测并依据管理员的指令执行修复动作。因此即使客户端系统无法与服务器通信或者是移动办公的用户，BigFix 客户端也可以自主工作，并通过预置的动作对系统进行修复和加固，确保客户端系统在离线的情况下也可以始终符合企业安全策略的要求。

7 公司介绍

BigFix, Inc 是全球领先的高性能企业级系统及安全管理软件供应商，提供业界唯一的可实现实时的系统生命周期管理，终端防护和安全配置及漏洞管理的统一管理平台。该平台可以帮助企业用户以全球规模实时查看，变更和执行 IT 策略。

BigFix 适用于高分布的，复杂的 IT 网络环境，借助于其单一的代理，统一的控制台，多样化的功能和按需部署的单一架构可实现实时的终端可见和控制。BigFix 的解决方案可以使用户更快速，更准确地对其全球 IT 架构进行安全管理，从根本上改善企业 IT 环境的治理，控制，可见性和业务能力。

BigFix 的产品及技术获得了业界和媒体的广泛认可，其获奖产品广泛地应用于政府部门、金融机构、服务提供商、医疗、教育，能源等行业用户及众多财富 500 强企业，拥有华尔街金融机构 65%的占有率。BigFix 产品目前管理着全球超过 7,300,000 台计算机系统。BigFix 的用户包括世界最大的零售商，世界最大的私营医疗机构之一以及中国铁路系统、中石化、中海油、中国人民银行、国资委、湖南移动、江西移动、广东政府、四川烟草等。更多信息请您访问 www.bigfix.com。