**虚拟化服务器的安全防护解决方案**

**背景**

廊坊银行数据中心存在的大量的虚拟化服务器，针对服务器的防护主要是前端边界的防护，而针对服务器端的防护手段很少，尤其是LINXU服务器在端点的防护为空白，无任何防护手段。因此廊坊银行需要一套安全防护措施来实现服务器端的基本安全防护。

**问题**

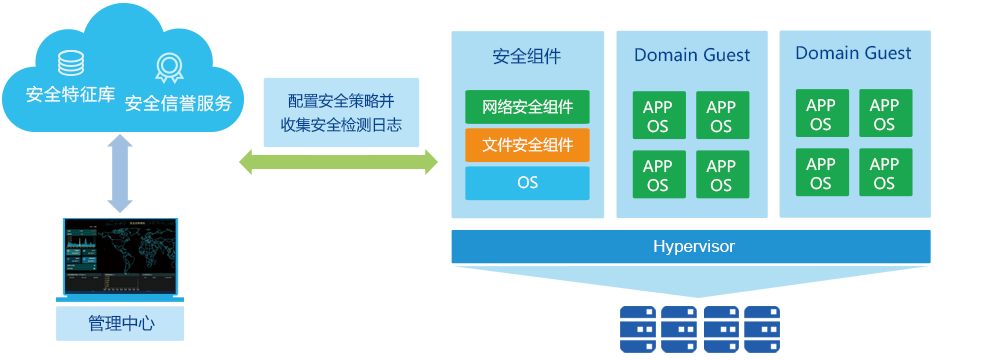
* 病毒防护：需要实现对服务器端的病毒防护
* 业务优先：以最简单易行的方式部署，减少服务器端的重启次数
* 虚拟化适应性：未来要实现同一控制台，来管理多虚拟化平台的虚拟机
* 网络适应性：银行数据中心有严格的区域隔离机制，控制台部署位置和被管理服务器无法直接通信
* 创新性：方案新颖，符合产业技术发展方向

**解决方案**

针对廊坊银行的虚拟化服务器防护需求，我司提供了提供“虚拟化安全”的安全解决方案，具体如下：

* 控制中心采用双代理模式部署，通过双层代理模式实现多区域的服务器管理及特征库的升级。
* 通过控制中心远程安装一体化客户端至虚拟主机上，实现虚拟主机防护病毒、虚拟主机防火墙等安全防护手段。

采用定时任务设置、任务并发设置、多升级服务器等优化功能，降低了启动、杀毒、更新等大并发动作对平台性能的冲击。



**价值收益**

* 统一管理中心，异构环境、统一管理。
* 通过双层代理的方式进行控制台的部署，成功解决网络不通问题
* 整个部署过程平稳升级，未对用户业务产生任何影响。
* 上线后多次成功阻断恶意攻击，服务器资产迄今为止无损失报告
* 虚拟化安全为用户提供灵活的安全功能扩展能力，可根据实际情况灵活选择安全能力