行业现状：

随着全球化不断扩展，创新的广度和深度不断扩展，金融行业信息化工作得到快速发展，规范、方便、高效、安全的金融业信息化服务体系初步建成。与此同时，金融行业对信息技术的依赖程度越来越大，特别是以综合业务系统整合、数据集中为主要特征的金融行业信息化发展到一个新的阶段。因而，信息技术风险也自然成为金融行业操作风险的重要方面。金融行业信息安全工作正面临比以往更严峻的形势，围绕信息网络空间的斗争日趋尖锐，网络违法犯罪活动呈快速递增趋势，恶意代码和网络攻击呈多样化局面，金融行业信息系统安全运行的难度持续加大，安全保障难度持续加大，给金融行业信息安全带来新的更大的挑战。

面临的挑战：

* 越来越多的金融企业都在把自己的业务网络化，例如开展网上银行业务，网上证券的买卖交易等。金融信息化的加速和信息网络化的推进将使金融信息系统内部采集、存储、传输、处理的信息量越来越大，信息的重要程度也越来越高。确保这些金融数据的安全采集、安全存储、安全传输和安全处理，将是金融信息系统建设面临的重要挑战；
* 金融信息化使得金融行业的客户资料转储为可被传播、利用以及共享的电子信息，频繁发生客户资料泄密事件，将严重影响金融行业企业的公众形象以及公信力。如何确保客户资料被安全、合理的授权使用已经成为越来越多金融行业企业所关注的重点；
* 随着金融信息化的加速，将使金融信息系统的规模逐步扩大，同时金融信息资产的数量也将急剧增加，如何对这些大量的信息资产进行有效的管理，使不同程度的信息资产都能得到不同级别的安全保护，将是金融信息系统安全管理面临的巨大挑战。
* 境内外网络违法犯罪活动呈快速递增趋势，新技术的应用使金融行业面临更大的挑战。金融业信息网络和重要信息系统正成为敌对势力、不法分子进行攻击、破坏和恐怖活动的重点目标。金融业信息系统已经遭受到多次攻击，整体信息安全形势严峻。

解决方案：

自动检查接入终端的安全状态，检查规则可自定义，检查内容包括：用户帐号、操作系统安全设置、防病毒软件状态、接入位置、终端的硬件信息等。

##### 依据接入终端的身份及安全状态，自动下发网络资源访问权限。

##### 自动隔离不安全的终端，并为其提供自助修复环境。

##### 自动发现接入终端是否受控，是否安装安全管理助手。

##### 对内部员工电脑、访客终端、外协人员终端分类管理；基于访客管理的网络准入无须客户端，并可实现访问时长、限定的访问控制列表，在特殊环境下还可跟短信网关联动。

##### 自动发现网络上的所有接入设备，并对设备进行定位。

##### 后台系统提供用户接入故障的原因、接入位置等信息，便于管理员维护。

客户价值：

实现对网络内部所有终端计算机接入进行网络准入控制，防止外来终端计算机或者不符合安全规定的终端计算机接入网络中；

实现对业务信息系统访问控制保护，建立业务数据访问控制规则，防止不符合安全规定的终端计算机接入到网络中