

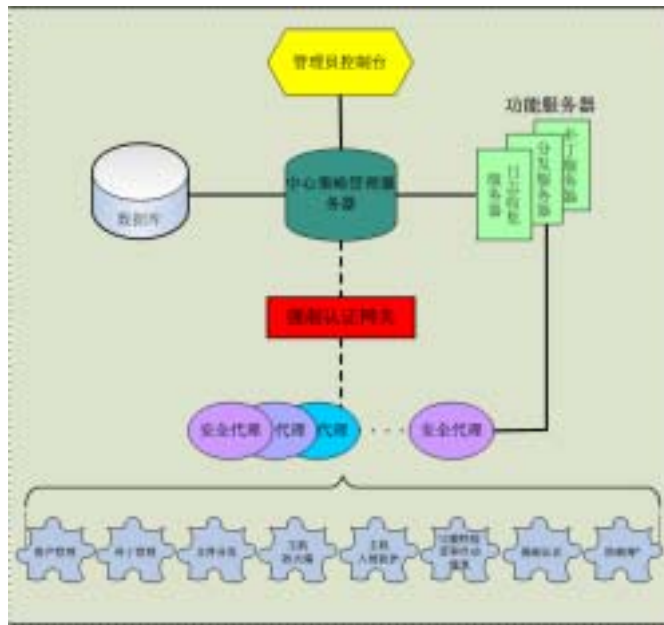
安氏终端安全管理解决方案——Terminal Guard

安氏着眼于企业安全管理中最为薄弱的终端管理的环节，推出了 Terminal Guard，该产品实现了以集中管理为基础的终端保护，以资产管理为核心的管理系统，它从企业内终端安全出发，核心思想是集中管理和强制，提供了基于 browser/server 和 client/server 相结合的全面终端安全管理解决方案，该方案具体提供了以下的功能：

- ◆ 资产管理
- ◆ 补丁管理
- ◆ 文件分发
- ◆ 主机防火墙
- ◆ 主机入侵防护
- ◆ 完整性检查和自动修复
- ◆ 强制认证

Terminal Guard 的体系结构

Terminal Guard 由六个主要的部分组成：安全代理、中心策略管理服务器、管理员控制台、强制认证网关、功能服务器（分发服务器，补丁服务器，日志收集服务器）和数据库。



Terminal Guard 的功能

◆ 资产管理

Terminal Guard 的客户端程序已经安装后，可以收集到各种信息资产，存放在服务器的数据库中，并不断跟踪终端的变化，从而保证管理员随时得到最新的信息，资产管理收集的信息包括各种硬件信息 - IP 地址、CPU、内存等，包括各种文件信息 - 安装的文件产品、补丁。

Terminal Guard 支持将计算机划分为特定的组，每个组可以拥有自己的策略，策略包括了补丁安装列表、文件安装列表、安全策略、完整性检查策略。

◆ 补丁管理

Terminal Guard 建立一个专门的检查机制用于检测补丁安装情况，安氏为每个补丁建立了一套特征，通过该特征可以检查补丁是否安装，目前这种机制能够检查 Windows 平台上的操作系统、IE、Office、SQL Server 等主流软件和补丁安装情况，保证仅仅安装需要安装的补丁。Terminal Guard 允许用户创建自己的补丁和补丁检查特征。

◆ 文件分发

支持从管理员控制台上传至 CPMS，再由 CPMS 分发到主分发服务器，由主分发服务器分发到所有从分发服务器，然后客户端可以检测并选择需要安装的文件。

◆ 主机防火墙

适用于多适配器环境，包括多条复杂的规则匹配条件。能够保存应用程序网络连接状态表，提供双向的状态检测功能，当发现未经学习的应用程序试图访问网络时，对其可执行映像路径、大小、版本、校验和等信息进行登记，记录的信息将由代理控制服务上报至中心策略管理服务器。

◆ 主机入侵防护

捕获进、出主机的网络数据包，进行基于签名的检测，并根据检测结果做出一定的响应。支持检测已知和未知的溢出攻击，可以通过捕获溢出成功后 Shell Code 在堆、栈上的执行，并及时终止攻击。对 Agent 主机上运行的所有或未授权进程的执行情况进行监控记录。

◆ 完整性检查和自动修复

支持自定义的完整性检查，允许指定检查某个程序的时间、大小、是否运行、HASH 等信息，保证企业的安全措施例如防毒、主机防火墙等系统有效保护用户并更新到最新版本。当某条规则规定的条件不满足时将自动执行完整性修复，手段包括执行本地某个文件或从指定 URL 下载并执行某个文件。

◆ 强制认证

强制认证模块是运行在强制认证网关中的一个访问控制模块。它作为外部的安全强制手段，保证被保护信息资产的安全。该模块根据安全代理提供的安全状态，被访问的地址及服务，及中心策略管理服务器提供的验证信息决定采取通过或阻止网络连接的动作。

Terminal Guard 的主要优势

- 最全面的企业系统管理和安全管理解决方案，融合 7 大功能，帮助客户打造高效率和高安全性的可信计算终端环境；
- 全模块化设计，按需购买和部署，具有极强的可扩展性，并且在不断开发新的系统管理和安全管理模块，可以做到平滑升级，切实保护用户的投资；
- 软件设计更符合中国企业的行政管理体制、财务管理和 IT 操作流程，并可以及时为大客户做按需定制。