



Terminal Guard 2.0
计算终端安全保障系统

FAQ

您可以信赖的**终端安全**管理专家

Creating more trusted cyberspace!

安氏互联网安全系统(中国)有限公司
Information Security One (China) Ltd.

目录

目录.....	2
1 什么是 TERMINAL GUARD.....	3
2 TERMINAL GUARD 的主要功能是什么.....	3
3 TG 的主要优势是什么.....	4
4 关于补丁管理.....	5
5 关于资产管理.....	5
6 关于集中管理.....	6
7 关于基于组的策略.....	6
8 关于完整性检查.....	6

1 什么是 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，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，该解决具体提供了一下功能：

- 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

2 Terminal Guard 的主要功能是什么

◆ 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，包括各种软件信息 - 安装的软件产品、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、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

支持将文件打包并分发给客户，通过自定义特征检查软件是否已经安装，并选择正确的安装参数和安装脚本。

◆ 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

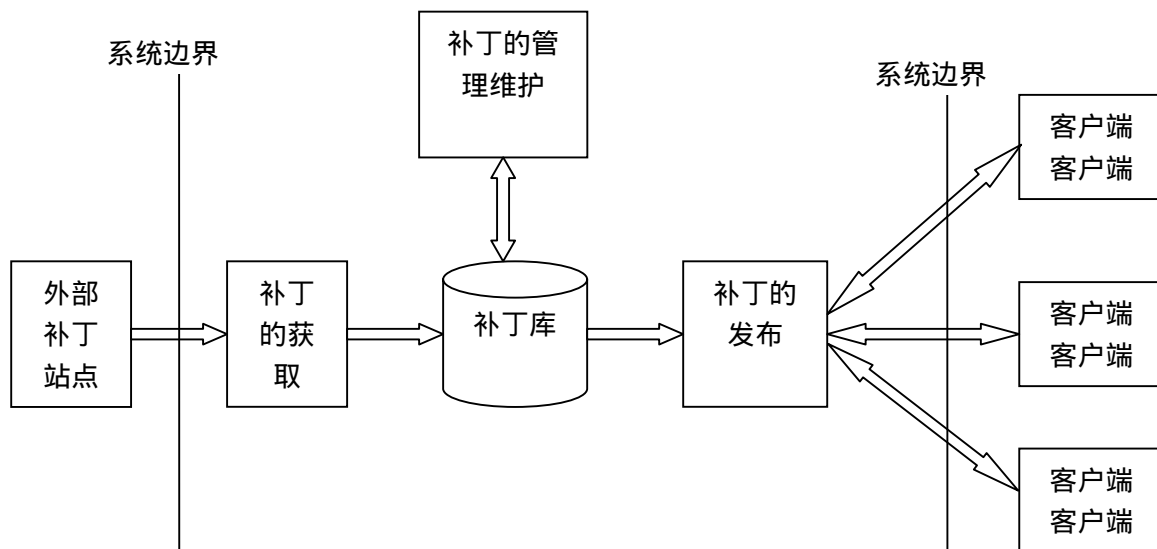
强制认证模块是运行在强制认证网关中的一个访问控制模块。它作为外部的安全强制手段，保证被保护信息资产的安全。该模块根据安全代理提供的安全状态，被访问的地址及服务，及中心策略管理服务器提供的验证信息决定采取通过或阻止网络连接的动作。

3 TG 的主要优势是什么

- 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。

4 关于补丁管理

软件及补丁管理子系统由补丁的获取、补丁库、补丁的维护管理和补丁的发布四个模块组成，



补丁获取模块负责从外部补丁站点获取最新的补丁更新。

补丁库模块负责保存所有软件及补丁的信息。

补丁的管理维护模块负责软件的添加和配置，补丁的验证和维护，补丁发布的策略等。

补丁的发布模块负责根据客户端的请求，返回相应的补丁信息。

5 关于资产管理

通过集中的方式对企业的所有终端进行全面的资产管理。Terminal Guard 资产管理具有如下的特性：

- 终端资产信息自动获取，大大降低了管理员的工作量，轻松掌握随时变化的终端资产状态。
- 集中的资产管理数据库，使得企业终端管理数据始终保持一致性。
- 组织结构视图、业务系统视图等灵活的管理方式增强了企业终端管理的灵活性和扩展性，更加符合中国企业的管理模式。
- 丰富全面的信息字段，覆盖终端信息的各个方面，完全符合大中型企业终端管理的需要。

6 关于集中管理

通过集中管理服务器，可以完成全部的终端管理工作。基于 B/S 和 C/S 相结合的服务器管理，更加增强了服务器管理的灵活性。资产管理、补丁管理、报表输出、数据库存储、日志存取与分析、权限分配与管理……等全部功能都可以通过集中管理实现，集中管理的机制，既有利于管理的方便性，又有利于企业的信息一致性管理。

7 关于基于组的策略

我们将组织结构中每个部门作为一个组，每个组可以拥有自己的补丁分发策略、文件安装策略和安全审核策略。

灵活的组划分策略可以保障企业依据自己的管理特点，按照部门、业务等不同的划分原则，定义不同的组，每个组可以拥有不同的补丁分发策略、文件安装策略和安全审核策略。

8 关于完整性检查

客户端的本地文件的完整性是是否出现安全问题的一个重要判断依据，管理员可以通过 Terminal Guard 管理服务器，设定相关的策略，按照 Windows 本地安全策略规则，定期检查某个特定文件的更改日期、大小和 hash。完整性检查完全符合 Windows 本地安全策略规则，符合 Windows 定义的标准。