

金融行业网站应用安全解决方案

根据金融行业网站系统现状及安全风险分析，智恒联盟应用安全团队通过对金融行业网站安全多年的研究、调研，针对金融行业网站安全提出了全新的安全防护方式，采用 WebGuard 网页防篡改保护系统解决金融行业网站安全防护问题免遭黑客攻击篡改，防患于未然，可以从根本上解决金融行业网站所面临的安全隐患，保障金融行业网站安全、稳定的运行。

系统组成

WebGuard 系统包含三个部分：监控代理客户端，管理中心服务器和管理客户端，各部分功能如下：

1. 监控代理客户端（Monitor Client Setup）安装在 Web 站点服务器上，根据服务器数量购买客户端数量，主要用于监控站点状态，执行管理中心所配置的策略；
2. 管理中心服务器（Center Server Setup）建议部署在独立 pc 服务器上，若所管理的 web 服务器数量较少，也可以同时部署在管理客户端；主要用于用户管理，策略下发，日志监控，以及管理各代理客户端；
3. 管理客户端（Console Setup）部署在网管员任意一台计算机，可以由单台 pc 机替代，主要用于登录管理中心服务器进行配置管理 WebGuard 中心服务器；



系统结构示意图

各组建之间通信采取完全加密传输，包括数据传输，用户认证等，确保通信的保密性；

系统主要功能：

- 基于驱动级文件保护技术，支持各类网页格式，包含各类动态页面脚本；
- 完全防护技术，支持大规模连续篡改攻击防护；
- 系统后台自动运行，支持断线状态下篡改监测；
- 驱动技术完全杜绝被篡改内容被外界浏览；
- 支持多站点分布式部署，统一集中管理功能；
- 支持大规模虚拟机、双机热备网站系统部署架构；
- 支持单独文件、文件夹及多级文件夹目录内容篡改保护；



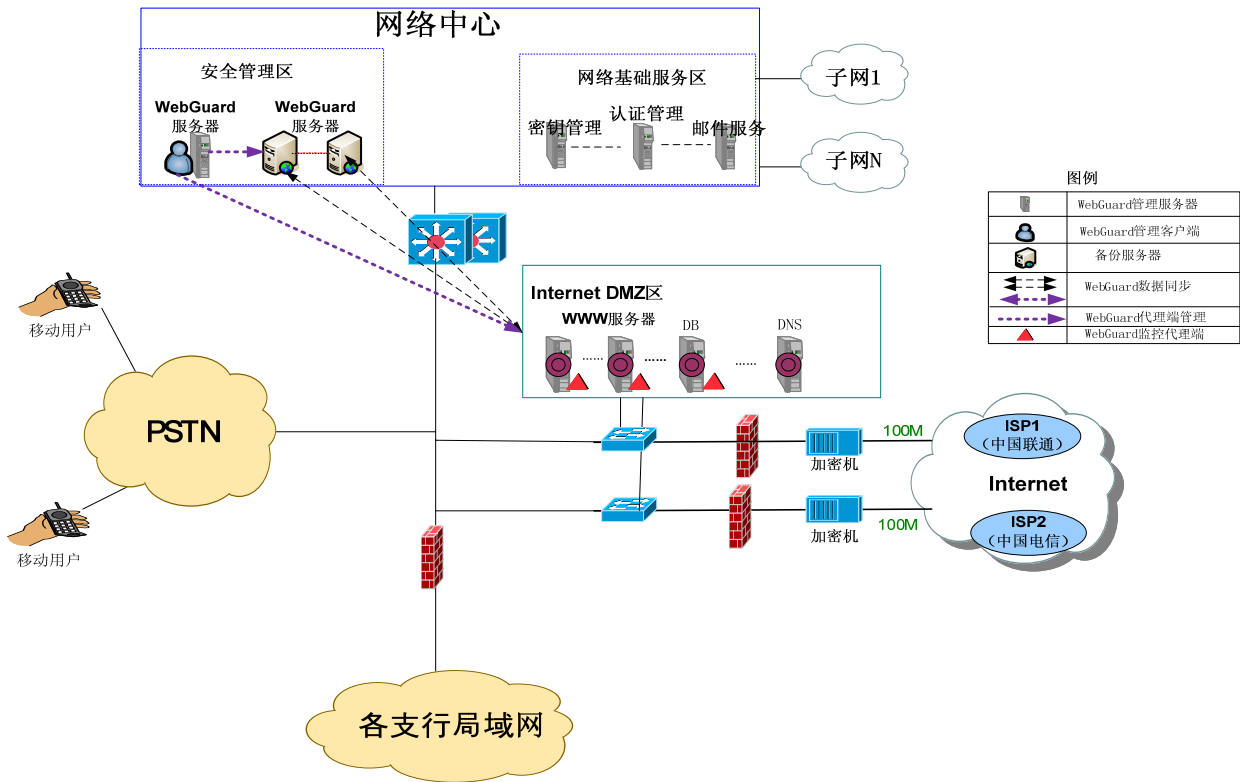
- 支持网页格式类型分类，便于分类管理；
- 支持网页自动上传功能，无需人工干涉；
- 支持异地文件快速同步功能和断点续传功能，极大的增加网站整体安全性和稳定性；
- 支持多用户管理功能，方便操作；
- 支持网页自动同步新增、修改、删除等功能；
- 自动检测文件攻击记录，并实时记入日志，支持导出excel报表；
- 支持服务器多种远程管理功能，如远程接管、远程唤醒、远程关机、远程用户注销等；
- 系统C/S结构，确保高可靠性；
- 支持多个策略管理，策略设置支持即时生效，无需重启；
- 支持服务器冗余双机及负载均衡分布部署；
- 支持多种告警方式，日志告警、声音告警、邮件告警或定制其他告警方式；
- 支持用户认证，采用加密传输，安全可靠；
- 系统全中文界面，操作、配置方便，网络管理人员仅需十分钟即可熟练完成系统初始配置，大大提高工作效率；
- 支持当前所有主流操作系统和web服务器。

网站动态自适应攻击防护模块主要功能：

- 支持SQL注入攻击防护；
- 支持跨站脚本攻击防护；
- 支持对系统文件的访问防护；
- 支持特殊字符构成的URL利用防护；
- 支持对危险系统路径的访问防护；
- 支持构造危险的Cookie攻击防护；
- 各类攻击的变种防护；
- 支持自定义检测库；
- 规则库支持在线升级功能；

技术特点：

- 完全基于事件触发机制，避免服务器资源额外开支；
- 文件驱动保护技术，确保系统稳定、安全、高效；
- 不限制网站发布服务器类型，实现高可用性和扩展性；
- 文件传输过程加密技术，防窃听和防篡改；



WebGuard 金融行业网站系统应用示意图

针对金融行业网站的复杂环境分析调研,通过在对外门户网站上部署 WebGuard 网页防篡改监控代理端,保护网站内容安全,防止网页遭到恶意篡改,同时在内容发布服务器或应用服务器上部署 WebGuard 管理服务器及可信代理端,用于网页内容同步、策略指定、日志收集,在中心管理区或教师用户区部署管理客户端(Console)用户远程登录管理,以上构架可以完全满足金融行业对网站内容防护的具体需求,有效保障金融门户网站的安全。