GHDN 应用防黑系统 2.0

产品白皮书

北京大唐高鸿数据网络技术有限公司

GOHIGH DATA NETWORKS TECHNOLOGY CO., LTD

二零一四年十月

信息更新

本文档及与之相关的计算机软件程序（以下称为文档）用于为最终用户提供信息，并且随时可由大唐高鸿更改或撤回。

文档版本：v2.0

发布日期：2014 年 10 月

适用范围：GHDN 应用防黑系统

信息反馈

如有任何意见或建议，请按如下联系方式反馈给大唐高鸿：

总部地址：北京市海淀区学院路 40 号研八楼

邮编：100191

电话：010-62303100

传真：010-62302575

免责条款

根据适用法律的许可范围，大唐高鸿按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，大唐高鸿都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使大唐高鸿确得知这些损失或损坏，这些损失或损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。

本文档中所有引用产品的使用及本文档均受最终用户可适用的特许协议约束。

GHDN 应用防黑系统白皮书

第一章安全概述

随着计算机技术和互联网技术的发展，有些用户环境也迁移至虚拟化环境、云计算中心，新的应用也层出不穷，与此同时，信息技术的发展也带来了安全威胁的发展。企业网络所面临的威胁在数量、种类和复杂性方面成倍增加，漏洞威胁成倍上升，受攻击频率越来越高，恶意代码变异越来越快；造成的危害越来越大。

常见威胁如病毒、间谍软件、木马软件、钓鱼程序、灰色软件、篡改数据、SQL 注入、跨站攻击等，涉及到网络层和应用层。

1. 蠕虫、僵尸病毒等网络层威胁，会造成：
   - 整个基础信息网络或者重要应用系统瘫痪，也可以导致大量机密或个人隐私泄漏，还可以用来从事网络欺诈等其他违法犯罪活动；
   - 种植广告软件，点击指定的网站；利用僵尸主机的资源存储大型数据和违法数据等，利用僵尸主机搭建假冒的银行网站从事网络钓鱼的非法活动；
   - 发送大量的垃圾邮件；
   - 从僵尸主机中。
2. 木马、间谍程序等应用层安全威胁，会造成：
   - 窃取用户的各种敏感信息和其他秘密，例如个人帐号、机密数据等信息并自动发送给病毒制造者；
   - 自动开启电脑上的某个端口，用于控制用户电脑；
   - 自动下载其他病毒程序，例如蠕虫病毒，用以控制整个计算机，对其他计算机用户发垃圾邮件、DDOS 攻击等；
   - 篡改文件，导致不良影响和经济损失等。

第二章产品概述

- GHDN 应用防黑系统是一款从网络层、应用层、操作系统层、文件层和管理层进行立体的预警防护的安全产品，能逐层排除安全隐患；系统从技术上、流程上和人员管理三个方面全面保障系统安全，降低整体安全风险。五层防护体系如下：

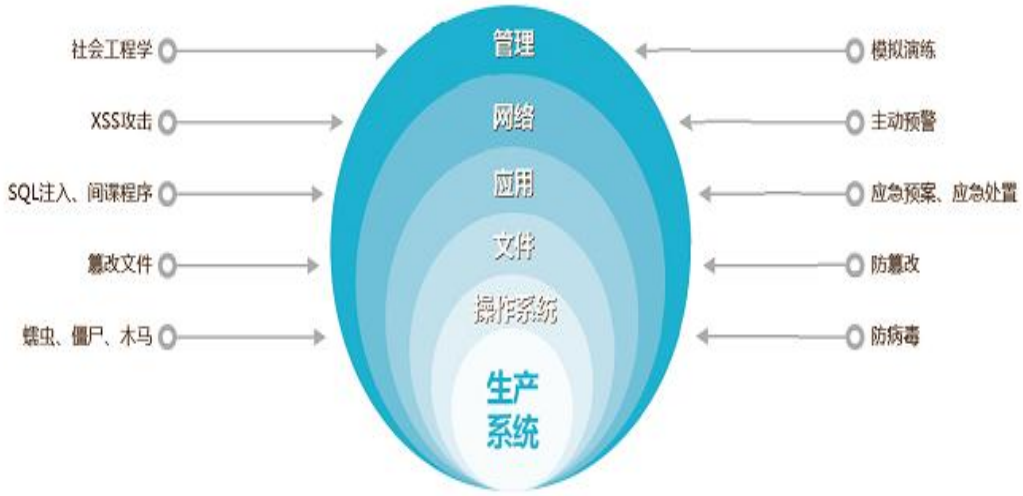


图 2-1 GHDN 应用防黑系统层次图

1、 文件层

- 针对网页文件采取防篡改的技术措施，以防网站页面被篡改而造成的不良影响；
- 采用非法手段欲篡改网页时，防篡改客户端能及时以邮件、声音等方式告警；

2、 应用层

- 针对来自互联网的常见的应用层威胁手段，合理利用网络资源，应采取有效措施，进行应用层恶意代码过滤；
- 防止 SQL 注入、跨站脚本攻击和其他 WEB 应用程序漏洞等。

3、 网络层

- 带有入侵防御功能、能过滤来自于网络层的攻击，例如：DDOS 攻击、缓冲区溢出攻击、端口扫描、暴力破解管理员密码等；
- 防止病毒、间谍软件、僵死、蠕虫以及其他恶意软件的侵害等。

4、 操作系统层

- 对操作系统进行漏洞探测，尽早发现威胁，提供漏洞防护。
- 收集操作系统日志，并进行分析，判断是否存在可疑行为和安全事件。

5、 管理层

- 提供严格的权限管理，登录认证管理。
- 提供管理员安全培训课件，提高人员安全技能。

■ GHDN 应用防黑系统为客户带来的价值：

- 多层次立体预警防护体系
- 集成多种安全防护技术
- 综合性的分析价值

- 策略联动
- 图形化监控

第三章系统架构

GHDN 应用防黑系统从多层进行立体防护，并采用主流的了 B/S 管理模式，由防黑客管理中心、恶意软件预警与防护端、应用预警与防护端端、完整性监控端组成了安全保障体系。防黑客管理中心可通过简单的设置进行级联，实现了针对复杂网络环境的无限扩展性安全体系，方便统一监控。

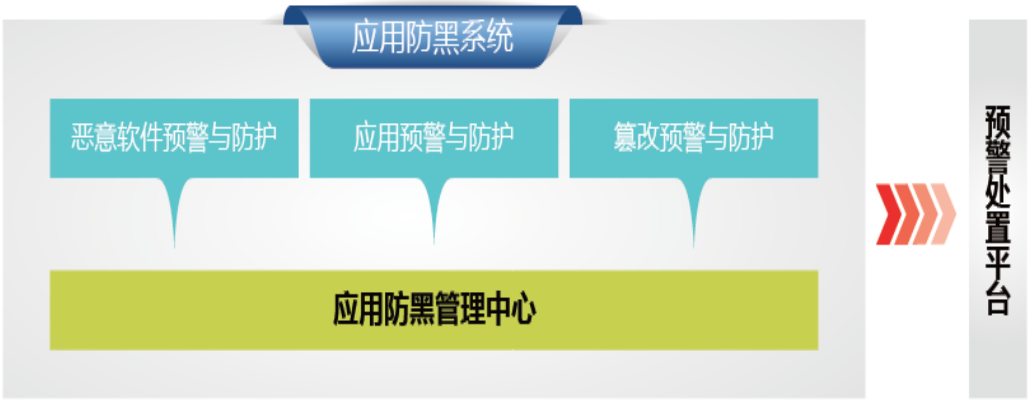


图 3-1GHDN 应用防黑系统结构图

1. 恶意软件预警与防护：

该组件部署在受保护的服务器或虚拟机上，用于实施数据中心的安全策略，发现和阻止针对操作系统和网络层的恶意软件，包括：

- 防止受病毒、间谍软件、木马和其他恶意软件侵害；
- 提供操作系统漏洞防护；
- 收集操作系统和应用程序日志进行分析，发现可疑行为。

2. 应用预警与防护：

该组件捕获网路数据，识别 WEB 应用威胁。该组件部署在 GHDN 应用防黑系统管理中心。识别如下威胁：

XSS 攻击、SQL 注入、远程文件包含攻击、系统命令注入、后门访问、PHP 注入攻击、HTTP 响应拆分攻击、HTTP 请求走私攻击、LDAP 注入攻击、元字符异常、会话固定攻击、SSI 注入攻击、EMAIL 注入攻击、远程文件访问尝试、系统

命令访问等。

3. 篡改预警与防护：
   该组件分三部分，保护端、同步端和策略管理端。
   - 保护端部署在受保护的 WEB 服务器机器上，运行有防篡改保护进程和驱动，进程以服务的形式运行。
   - 策略管理端主要是管理各个受保护机器的用户和密码，管理受保护的网站和对应的机器，建立保护策略，指定网站下的哪些目录和文件受保护。
   - 同步端监控用户更新的文件，向 WEB 服务器上同步修改的文件和目录。

4. 防黑客管理中心：
   - 防黑客管理中心是 GHDN 应用防黑系统进行信息管理和预警防护的控制核心。防黑客管理中心与其他子系统通过通讯方式连接，与其它子系统在管理中心控制下完成协同工作。
   - 通过数据库技术，系统中心可以实时记录 GHDN 应用防黑系统内被保护服务器上的恶意软件防护信息、文件完整性监控信息和应用预警防护以及服务器系统日志。
   - 防黑客管理中心综合分析记录的安全事件，进行威胁预警。
   - 防黑客管理中心具备级联功能，可以向上级中心上传数据。
   - 同时，系统集成了基于 WEB 方式的控制台，整个多层次的解决方案，都能够通过集中管理平台进行统一管理，策略配置和报表制作。此控制台界面结构友好、直观；通过具有基于角色的管理策略，进行分级和精细管理。

第四章主要功能

1. 防止恶意软件

防止服务器受病毒、间谍软件、木马和其他恶意软件的侵害。实时检测并移除服务器中的恶意软件。阻止试图通过卸载或中断安全程序避开检测的恶意软件。检测可疑或恶意活动并发布警报。

2. 篡改预警与防护

监控关键的操作系统和应用程序文件（如目录、注册表项和值），以便实时检测并报告恶意的更改或意外的更改，设置策略。

3. 应用威胁预警防护

检查所有输入和输出通信，防止 SQL 注入、跨站脚本和其他 WEB 应用程序漏洞。

4. 操作系统防护

为操作系统提供立即可用的漏洞防护，并收集操作系统和应用程序日志进行分析，以确认是否存在可疑行为。

5. 安全管理

通过管理中心，进行集中管理、集中设置、集中维护。系统集成了基于 WEB 方式的控制台，整个多层次的解决方案，都能够通过集中管理平台进行统一管理，策略配置和报表制作。

6. 安全预警周报

每周提供安全预警报告，总结本周安全状况，并提出安全应对策略。

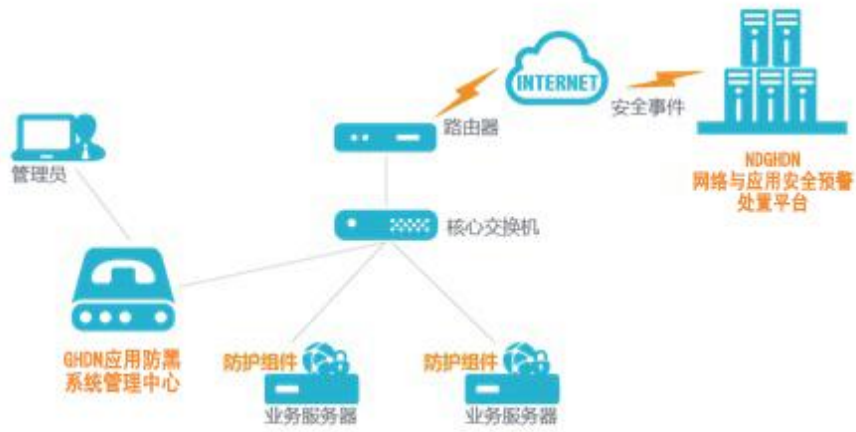
7. 多途径报警机制

管理员可以通过 SYSLOG 事件日志、Email 等多种方式接收安全事件报警，以保证及时应对安全事件。

8. 图形化监控

系统将安全事件已图形化方式呈现出来，以便于管理员分析安全发展趋势，并采取针对性的措施。首页对整体概况以及重点监控对象进行展示。

第五章系统部署



GHDN 应用防黑系统由系统管理中心、恶意事件采集组件和防护组件组成。

第六章服务体系

大唐高鸿的基本服务条款：

1. 售后服务

- 提供 1-5 年设备维保服务
- 提供现场和远程技术支持
- 技术支持邮箱：service@gohigh.com
- 联系电话：400-707-8778

详见<<售后服务条款>>

2. 可选安全服务部分

详见<<大唐高鸿安全服务体系>>