天擎终端安全管理
解决方案

目录

背景

随着企业信息化进程的不断加快，企业网络规模与终端数量在不断变大，企业业务对信息化系统的依赖程度越来越高，信息化系统的建设与升级，一方面推动着企业的办公自动化、业务自动化进程不断加快，提高企业的运营效率，降低企业的运营成本。另一方面，也为企业带来了新的问题，对企业的运营与管理提出了新的挑战。

- **管理问题**

  信息化系统的引入、网络的建设与升级为企业带来了诸多管理问题，其中主要包括如下几个方面：

  - 如何有效管理网络设备与应用系统，使得网络能够稳定运行，保障企业自动化办公与依托于网络的业务能够平稳有效进行，这需要大量额外的网络管理系统进行运维支撑。
  - 如何有效管理终端设备与应用软件，使得终端能够稳定、合规运行，保障企业的自动化办公与终端业务操作能够平稳有效进行。
  - 如何有效管理业务系统的设备与软件，使得业务系统整体平稳运行，保障企业业务系统对外提供稳定的服务。

- **安全问题**

  信息化系统与网络的引入，为进入企业内部获得企业数据资料、操控企业业务运行提供了一种看不到的新途径，这就为企业的数据、资料乃至业务运行带来了新的安全问题，主要包括：

  - 企业信息化系统与网络访问控制问题：这其中包括如何控制哪些终端在满足什么样的条件之下可以进入到企业信息化系统与网络；如何为进入到信息化系统与网络的终端用户分配访问操作权限并保障这些终端用户不能越权非法操作。
  - 信息化系统及其支撑设备的安全运行问题：这其中包括如何保障信息化系统及其软硬件系统不会受到攻击，或者在受到攻击的情况下可以有效避免损失、缓解攻击带来的影响、保障信息化系统与网络仍能够安全、可靠、平稳地对外提供服务。

- 企业数据及资料的安全问题：这其中包括如何保障企业的数据及资料能够安全存储、安全访问，对于这些企业数据与资料要做到：非授权人员拿不到、非授权人员拿到后带不走、非授权人员拿走后打不开等三个层次的安全防护。

- **评估问题**

近些年，随着我国信息化系统的大范围建设与普及，信息化系统的建设已经进入到快速发展期，大多数企业的信息化系统与网络已经从初期的从无到有发展到了现在的颇具规模，相应地，在信息化系统的建设上，企业也开始从最初的基础设施建设逐步进入到了信息化系统稳定运行的收获期。更进一步，很多企业也已经开始理性思考在信息化系统上的大量投资带来的具体企业效益，换句话讲，企业的信息化系统已经进从基础设施建设发展到了建设效果评估阶段，科学评估信息化系统建设的成果，向信息化系统建设要效益是这个阶段的主要目标。

方案目标

本方案的目标是从企业信息化系统终端安全与管理的角度出发，以终端安全为核心，以终端桌面管理为重点，提供以终端为基础的桌面安全与管理整体解决方案，具体内容包括终端安全、桌面管理、统一运维三个方面：

终端安全

提供针对终端安全的防护措施，为终端提供安全的上网办公环境，具体包括如下几方面内容：

- ✓ 终端病毒与恶意代码防范
- ✓ 防黑加固
- ✓ 主机防火墙
- ✓ 终端安全性检查

桌面管理

- ✓ 终端流量管理
- ✓ 系统自动升级
- ✓ 终端远程协助
- ✓ 终端硬件性能监控
- ✓ 终端进程与服务管理
- ✓ 终端 Agent 强制安装与运行
- ✓ 终端外设管理
- ✓ 终端小工具
- ✓ 终端信息搜集
- ✓ 文件审计管控

统一运维

- ✓ 软件分发
- ✓ 策略下发
- ✓ 在线用户统计
- ✓ 安装包定制与 Web 安装
- ✓ 系统可扩展能力
- ✓ 系统容灾

方案设计

终端安全

终端病毒与恶意代码防范

在这一部分中，将就与终端安全相关的检测与防御方法进行方案级描述，将主要涉及两方面与终端密切相关的内容：

- ■ 终端病毒防御

■ 终端数据的安全防御

终端病毒防御

该功能的目标是对互联网中的病毒、木马、蠕虫、网马、僵尸网络、流氓软件、间谍软件等恶意代码进行有效的识别、查杀与隔离

功能框架

本方案对病毒、木马、蠕虫、网马、僵尸网络、流氓软件、间谍软件等恶意代码的识别和查杀采用了多套高性能检测引擎的技术方案，这些技术方案中，既包括传统基于静态病毒特征的多模式匹配的检测技术、也包括无特征的人工智能检测技术和基于云端的云查杀检测技术，多种检测技术的综合运用，最大限度地保障检测的有效性，具体来说，本方案中采用了如下几种关键的检测技术：

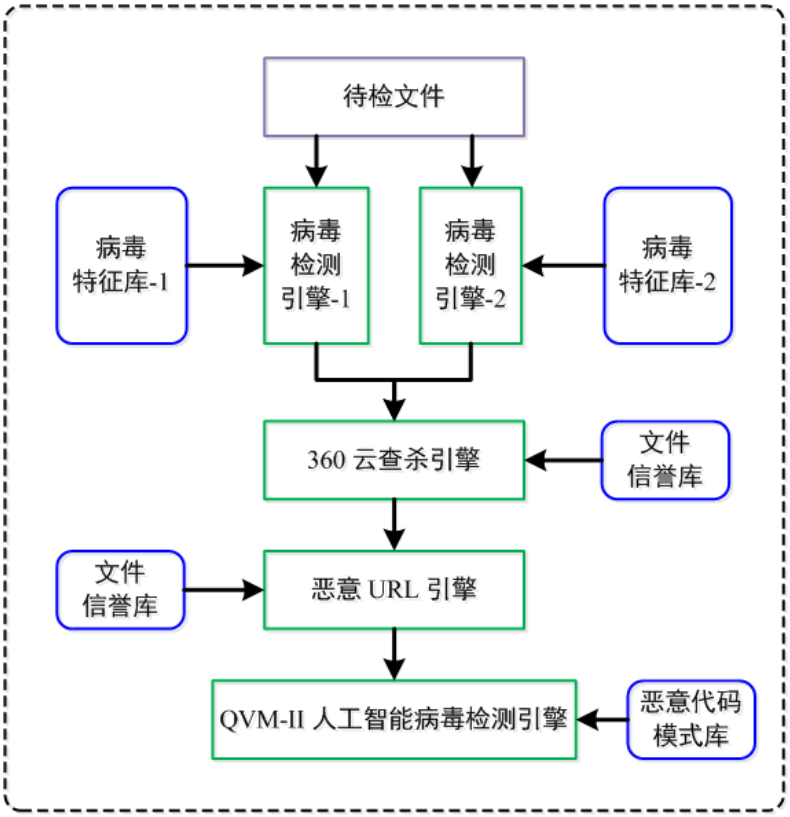
① 双病毒检测引擎

② 云查杀检测引擎

③ 恶意 URL 检测引擎

④ QVM-II 人工智能检测引擎

已知病毒查杀功能框架如下图所示：



方案说明

双病毒特征库与双病毒检测引擎

与其他病毒检测产品不同，本方案采用了双引擎的查杀技术，具体来说就是采用实现技术完全不同的两套独立的病毒库、病毒检测引擎对已知病毒进行检测。因为已知病毒检测的关键是病毒库的覆盖度和检测引擎的预处理能力，因此如果其中一套病毒检测引擎出现错误（误报、漏报）的可能性为 P（P < 1），另一套病毒检测引擎出现错误（误报、漏报）的可能性为 Q（Q < 1），那么两套完全独立的病毒检测引擎同时出现错误（误报、漏报）的可能性就是 P Q（P Q < min(P, Q)），举例来说，如果第一套引擎出错的可能性是 P = 2%，第二套引擎出错的可能性是 Q = 3%，那么两套引擎同时出错的可能性就是：

(0.02) (0.03) = 0.0006

可以看到，双病毒特征库，双病毒检测引擎的方案，与单病毒库、单病毒检测引擎相比，在检测的准确率上有大幅提升，由于双病毒特征库，双病毒检测引擎与单病毒库、单病毒检测引擎相比，性能开销（CPU 消耗、内存消耗）会更大，

因此本方案中对是否启用双病毒库、双病毒检测引擎采用了配置开关，可以根据终端硬件的配置情况灵活启用或者关闭该功能。

云查杀检测引擎

➢ 云查杀技术的必要性

随着病毒的大量出现，传统的本地病毒库的查杀方式已经无法在本地加载绝大多数病毒样本特征，仅奇虎 360 一家安全企业，到目前为止就已经积累了多达 20 亿的病毒样本，如果算上未经去重的病毒样本，目前已发现的病毒样本已经远远超过 20 亿的规模，而目前大多数的终端杀毒软件，受本地存储资源的限制，本地病毒特征库的规模大约在 1000 万 ~2000 万左右，这个数字只占不到 20^{+} 亿已发现病毒样本的 1%，依靠 1%的病毒库去检测互联网中肆虐的病毒，这说明传统的本地病毒库的查杀方式已经无法满足对已知病毒的查杀要求，需要通过云端的海量计算资源与海量存储资源满足对数十亿病毒进行 100%查杀的安全需求。

➢ 云查杀资源与技术

云查杀技术需要大量的样本资源、计算资源、检测技术资源，如果没有这些资源作支撑，则无法构建高质量的云查杀系统，本质上来说，云查杀系统是一个海量资源系统，这个资源系统中，既包括客户资源，又包括硬件资源与软件算法资源：

- 样本资源

  构建云查杀系统，需要海量的病毒、木马、僵尸网络等恶意代码样本作为资源支撑，否则，所构建的云查杀系统将因为缺乏足够的病毒样本积累而难以保证对于已知病毒和恶意代码的检测率。本方案中，我们采用的 360 云查杀平台，拥有涵盖了近 20 年的所有已知的病毒、木马、蠕虫等恶意代码的样本文件，其所积累的去重之后病毒样本数量已经超过 20 亿。

  样本资源的基础是客户资源，没有足够的客户资源作支撑，无法收集足够的病毒样本文件，只有广泛部署了终端系统的情况下，才能在短期内收集足够数量的恶意代码样本文件，奇虎 360 在全国拥有超过 4 亿的终端用户，覆盖了全国终端用户的 95%以上，其中绝大多数已经选择加入

了奇虎 360 公司的“云安全计划”，这些遍布全国的海量用户为 360 提供了丰富、及时的病毒样本资源，保证了 360 云查杀系统病毒样本收集的及时、有效。目前平均来说，一个病毒从首次在国内互联网上出现，到被 360 云查杀系统捕获之间，只有不到 10 个小时的时间。

- 计算资源

  为了构造有效的云查杀系统，需要大量的计算资源进行支撑，以便对搜集到的样本资源进行深入分析，一般来说，一台标准的服务器（如 DELL R720，配置为：双路 16 核 CPU（Xeon E5-2690，单路 8 核，主频 2.9GHz）、Intel C600 主板芯片组、内存 16GB（ECC DDR3）、硬盘 900GB（SAS 接口）），每天（24 小时）可处理的样本数量大约在 3000 万个左右，因此，对于标准 1000 终端的用户来说，若按照每天每台终端提交 10 个样本进行深度检测，则大约需要 4 台 DELL R720 这样配置的服务器组成的云查杀系统才能满足查杀需要。在本项目中，360 所提供的云查杀系统的规模已经超过了 10000 台服务器，由这些云服务器所构成的查杀环境，完全可以满足本项目的云端深度查杀需求。

- 算法资源

  构建有效了云查杀环境，除了稳定、及时的样本收集资源与足够数量的硬件计算环境之外，还需要先进的未知病毒及恶意代码的检测算法，这样才能够在收集到病毒与恶意代码样本之后，进行有效的分析与处理。因此，对未知病毒与恶意代码的快速检测能力，就成了构建有效的云查杀环境的关键。在本方案中，360 所提供的云查杀环境集成了大量先进的真对未知病毒与恶意代码的查杀算法，这些算法中，有基于病毒与恶意代码静态样本共性特征的 QVM-II 算法（该算法采用人工智能与机器学习的方法，对 360 目前已经积累的 20 多亿病毒样本进行多次切片学习，抽取出病毒与恶意代码的共性特征，建立恶意代码的不同族系模型，该算法在北美、欧洲的多项恶意代码检测能力测评之中名列第一），也有目前主流的动态沙箱深度分析技术，同时还集成了利用未知漏洞进行病毒与恶意代码传播的基于内存分析的动态漏洞利用攻击分析技术，最后，对于非常复杂、难于分析的可疑文件，还会采用具有多年病毒分析

与对抗经验的专家分析团队进行彻底分析。以上这些先机的自动化分析技术与方病毒专家团队人工分析的有效结合，多种手段、人机结合，保证了对病毒与恶意代码分析的万无一失。

- 360 云查杀隐私问题说明

由于本方案中采用了云查杀技术，云查杀技术需要在终端与云端之间交互必要的样本数据以保证对样本进行有效检测，因此需要对云查杀过程中终端与云端之间所交换的数据进行详细的说明，以此排除隐私泄露的可能。

360 公司承诺并保证：在使用 360 云查杀系统的过程中，除了必要的检测之外，不会以任何形式非法采集、利用用户的任何隐私数据，下面进行逐一说明：

1、云查杀系统的使用完全由终端用户自行决定，可以由管理员统一配置，如果终端用户或管理员选择关闭云查杀功能，则终端将不会向云端传送任何检测所需要的数据进行病毒与恶意代码的检查

2、对于云端深度检查，终端和云端之间也只会传送可执行文件（PE 格式），而不会传送敏感的数据文件（如：word、pdf、图纸、图片等），因为只传送了可执行文件，可执行文件只是程序的执行体，有可执行代码组成，并不包含用户的敏感数据，更不包含用户的隐私信息，因此不存在隐私泄露或泄密的可能

3、对于云端非深度检查，终端和云端之间连可执行文件都未进行传输，而只是抽取了可执行文件（PE 格式）的部分属性信息（而非可执行文件体）传送至云端进行检查，这些文件的属性信息与文件内容完全无关（就如同一个人的姓名、居住地、职业信息与这个人的血型毫不相关是同一个道理），因此在非深度的一般性云查杀中，理论上就不存在隐私泄露的可能性。在非深度云查杀的过程中，终端与云端交互的文件属性信息包含且仅包含如下内容：

- ✓ 该文件在终端的存放路径
- ✓ 该文件的哈希指纹（MD5、SHA-1）
- ✓ 该文件的大小
- ✓ 该文件所在终端的操作系统类型
- ✓ 该文件所在终端的操作系统版本号
- ✓ 该文件所在终端的 IE 版本号

4、所有云端与终端之间的交互的信息，除了需要深入分析的不含用户任何数据信息、隐私信息的可执行文件可能会涉及到专家人工分析之外，其余的所有信息将完全由机器进行自动处理，除了检测之外，没有任何渠道可以获得这些信息，所有的过程都是有机器完成，即便是不包含用户隐私的文件属性数据，除了机器之外，也不会有其他的途径可对之进行提取和阅读。

以上就是在本项目中所采用的 360 云查杀系统的隐私问题的说明，可以看到，采用 360 云查杀系统完全不存在任何用户隐私的泄漏问题。

恶意 **URL** 检测引擎

Web 应用是目前互联网的最主要应用，Web 安全问题因此也成了互联网安全问题中最重要的问题，占据了互联网问题中的绝大部分，网银诈骗、网购诈骗、钓鱼网站、网马等通过恶意网址进行钓鱼、诈骗、侵财的攻击事件频发，已经成了 Web 应用的主要威胁，同时也发现，部分 APT（高级持续性威胁）攻击行为也是通过恶意网站（一般是钓鱼网站）对企业低权限终端进行入侵，进而以此低权限终端做跳板不断渗透高权限终端与服务器，最后完成 APT 攻击过程，因此对于访问 Web 过程中的安全防护，已经成了当前终端安全防护的重要组成部分。

从技术上来看，对于终端访问恶意网址的防护主要有三种技术手段：

1、实时分析、动态检测

2、事先分析、静态匹配

3、实时分析结合事先分析，动态检测结合静态检测

第一种技术手段完全依靠在用户访问 Web 过程中对页面及其附属资源的动态分析和主动防御技术（如：IE 控件监控、内存监控、注册表监控）等方法对用户访问恶意网站、恶意链接的行为进行发现和阻断。这种方式的优点是可以对恶意访问行为进行实时发现，但其缺点也比较明显，即：如果对用户访问的 Web 访问进行深度分析，会消耗大量的用户本地资源，如果分析结论的得出也可能需要完整的分析过程之后才能完成，此时可能攻击行为已经部分发生，同时，完全依靠本地的动态分析，也存在一定的漏报可能，这些都是单纯依靠实时分析、动态检测可能会出现的一些问题。

第二种技术手段本质是通过云计算的方式来完成的，即：事先对互联网中存

在的链接进行采集，采用动态分析结合沙箱的方式进行事先检测，将存在恶意行为的链接形成静态恶意链接库，终端在访问一个链接之前，终端系统安全代理会将此链接与恶意链接库进行比对，如果发现此链接在恶意链接库中出现，则认为该链接属于恶意链接，进而对其访问行为进行禁止，与单纯蚕蛹实时分析、动态检测的技术相比，采用这种方法可以大幅度降低终端的资源消耗，可以在第一时间发现恶意链接（而不是等整个页面及其资源文件都下载到本地并进行了分析之后），同时由于依靠云端的事前抓取分析、云端用户的检测结果，漏报的可能性非常小。但这种技术也存在一定的局限性：对于新出现的恶意链接，因为还没来得及被云端抓取分析，因此在一定时间内（比如：30 分钟）对这类新出现的恶意网址无法提供检测能力，即会出现漏报；另一方面，对于被挂马的受害网址，如果木马被清除，那么短期内（在下一轮抓取完成之前），该网址仍将被列入在恶意网址库之中，即在这段时间内会有误报出现。

第三种技术是结合上述两种方法，这种方法优势非常明显，即：对于大多数白名单中的网址直接放行，对于黑名单中的网址直接拦截，对于灰名单（即没在白名单、也没在黑名单）中的网址则采用动态分析、主动防御技术进行实时分析。这种方式的优点非常明显：既利用了云端与其他终端的检测结果过滤了大量的白链接、拦截黑链接，大幅降低了客户端的资源开销，同时对极少量稀有链接又利用动态分析、主动防御技术进行深入的动态分析，起到了查缺补漏的效果。

在本方案中对于恶意 URL 的检测，采用的是第三种方法，即：动态分析结合静态匹配的技术方案，通过上述的技术分析可以看到，可以清晰地看到，本方案可以满足对恶意链接的精确检测要求。

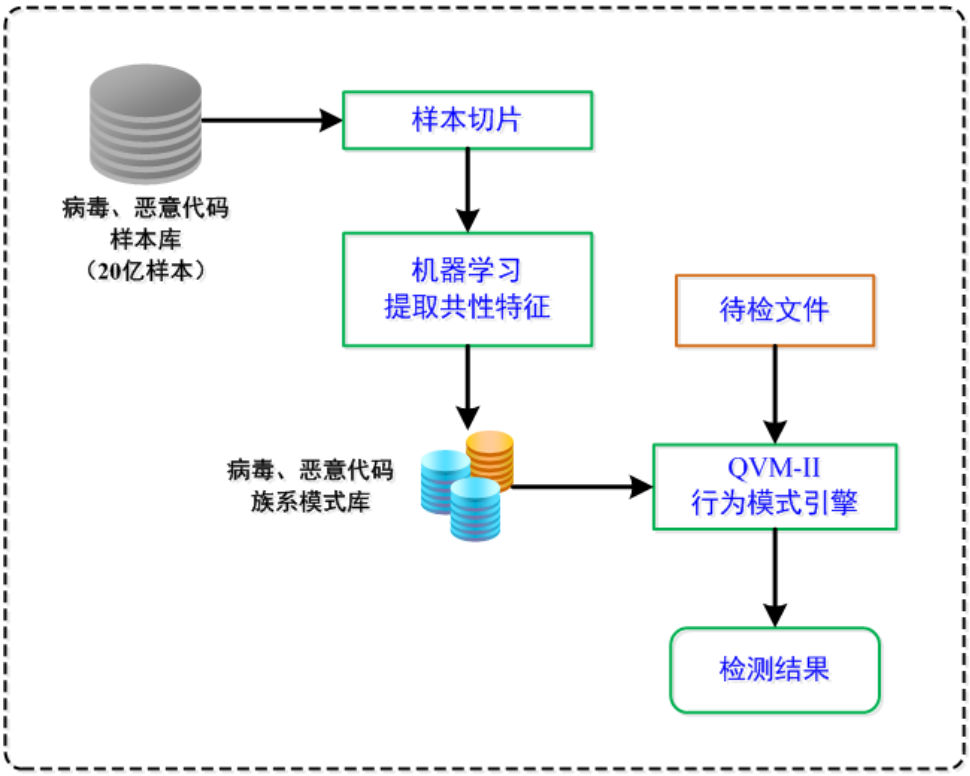
QVM-II 人工智能检测引擎

对于病毒和恶意代码的检测，一直存在着两个技术方向，一个是依靠病毒特征匹配的静态检测技术，这种技术的特点是必须依靠已知的病毒特征，一般静态特征匹配的技术适合对已知病毒、恶意代码的检测。另外一种是依靠对病毒行为的动态分析技术，这种技术更适合对未知病毒、恶意代码的检测。这两种技术是目前对病毒进行检测的关键技术，分别实现对已知、未知的病毒及恶意代码检测。

其中采用特征对病毒进行检测的技术又分为两个方向，一个是穷举式病毒特征提取，即针对每个已发现的病毒、恶意代码样本提取各自的病毒特征，这种方

式的优点是能够准确识别出已提取特征的病毒与恶意代码，误报率和漏报率都很低。另一种是针对不同族类的病毒及恶意代码提取出共性的族群特征，并以此作为检测依据对恶意代码进行检测。这种方式的优点是不依赖某一个病毒或恶意代码的具体特征，而是提取某一族群的恶意代码共性特征，因此，这种检测方法对于某一病毒与恶意代码族群内的新生病毒具有非常强的检测能力，同时还能对检测出来的病毒与恶意代码进行族系归类。

QVM-II 人工智能检测引擎采用人工智能与机器学习的方法，对目前已经积累的 20 多亿病毒样本进行多次切片学习，抽取出病毒与恶意代码的共性特征，建立恶意代码的不同族系模型，该算法在北美、欧洲的多项恶意代码检测能力测评之中名列第一。该技术的主要组成框架如下：



终端安全性检查

■ 目标描述

根据终端的安全状况，决定其是否能接入到网络之中，亦即将终端的安全状况作为网络准入的前判断件之一。此功能的最终目的是强制终端落实规定的安全

防范措施，进行安全加固工作，隔离可能成为安全短板的终端。

■ **设计描述**

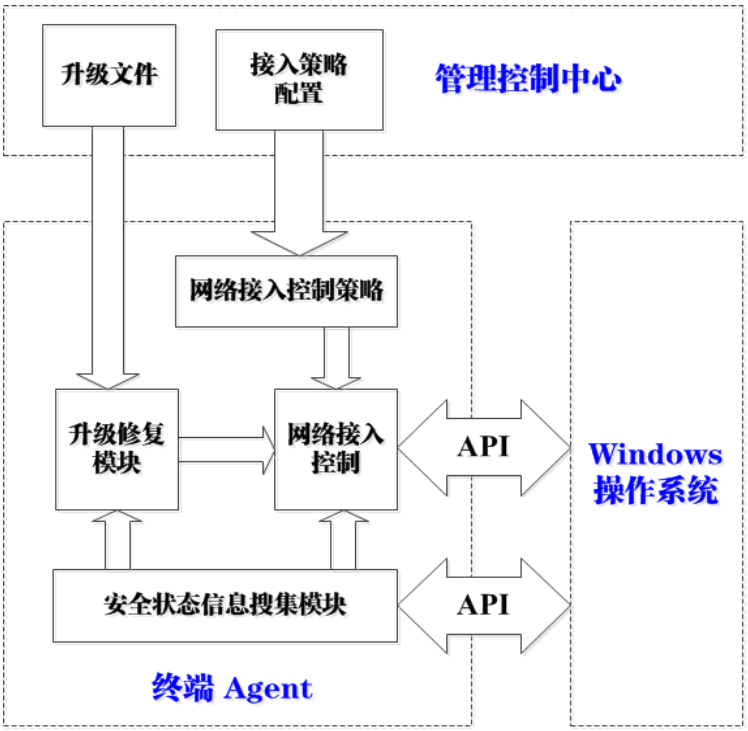
本功能由 4 项子功能组成：

- 子功能 1：终端安全状况信息收集（包括：当前终端的登录账号、当前终端的杀毒软件安装与运行情况、当前终端杀毒软件病毒库的版本信息、当前终端操作系统的安装情况）。
- 子功能 2：病毒特征库、系统漏洞补丁文件自动下载、自动修复。
- 子功能 3：根据策略阻断终端连入网络。
- 子功能 4：通过管理控制中心配置终端安全状况准入策略，支持按照 IP 地址、网段、IP 地址区间下发到不同的终端。

终端安全状态的几个关键指标是：

- ✓ 登录账号是否合法。
- ✓ 是否安装并运行了规定的防病毒软件。
- ✓ 病毒库是否升级至最新。
- ✓ 操作系统补丁是否升级至规定标准。
- ✓ 硬件是否变更。
- ✓ 是否存在非法外联的现象。

说明：对于子功能 1 中的杀毒软件的病毒库的安装情况以及杀毒软件的病毒库版本情况的检查，将锁定在有限的几家杀毒软件（如：瑞星、金山、卡巴斯基、诺顿、MAcfee、趋势科技等），如果需要检查其他厂家的杀毒软件，则通过额外定制开发完成。



终端防黑加固

■ **目标描述**

对客户端进行防黑加固功能，提供有针对性监控功能，包括系统账号变更、重点端口监控，共享目录管控等。

■ **设计描述**

① 对终端密码复杂度、生存期和密码历史进行检查，如客户机不满足将提示终端用户修改；

② 对重点端口进行监控，并支持自定义端口监控与上报；

③ 可以显示终端开启的共享目录并对共享目录进行管理（关闭共享）

④ 可监控用户账号权限发生变化；用户组权限发生变化；用户账号增加、减少；用户组增加、减少；用户账号状态发生改变（启用、禁用），同时上报日志

协议防火墙

- **目标描述**

在内网终端间建立访问控制机制，杜绝非业务需求下的终端互访现象，遏制网内主机发起的攻击。

- **设计描述**

① 基于 IP、端口双向配置基于主机的访问控制策略。实现同个子网或不同子网内终端之间的访问控制，在不需要对原有网络设备做任何调整的前提下，实现细粒度的安全域访问控制管理。

② 可禁止终端 PING 出、PING 入，有效遏制内网嗅探行为。访问控制策略在控制中心集中定义，可根据不同分组按需下发，分布式执行，简洁、高效。

桌面管理

终端流量管理

- **目标描述**

对客户端访问外部子网的流量进行统计与限制，实时统计全网内各客户端访问流量的排名。

- **设计描述**

流量访问策略配置

③ 在控制端提供 TAB 页面，对终端/终端组（可通过 IP 地址、IP 区间、子网对应）访问目标网络或目标服务器（可通过 IP 地址、IP 区间、子网对应）的网络流量（速率）上限进行配置（最小单位：KBps）。

② 此配置作为策略下发至各个终端。

终端访问流量计数

④ 终端在网络层统计各自访问的流量，包括：

- ✧ 该终端的总体访问流量速率。

- ✧ 对特定目标主机的访问流量速率。
- ✧ 对特定子网的访问流量速率。

④ 终端将各自的流量统计数据上报至管理控制中心。

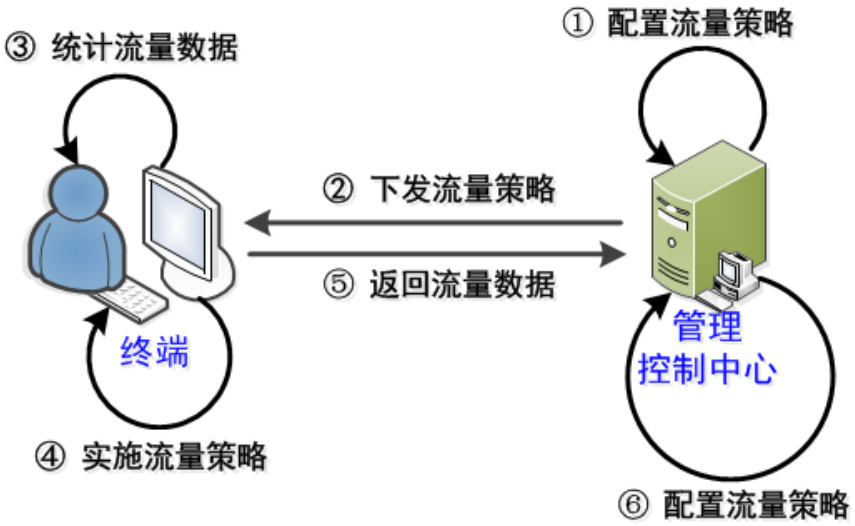
终端访问流量控制

⑤ 根据管理控制台为该终端下发的流量控制策略与终端统计出的当前的访问流量，对该终端的流量速率进行整形限制，注意，此处需要根据流量访问策略区分如下三种情况进行流量限制：

- ✧ 对该终端的总体访问流量速率进行整形限制。
- ✧ 对该终端与特定目标主机的之间的通信流量速率进行整形限制。
- ✧ 对该终端与特定子网的通信流量速率进行整形限制。

全网流量统计排名

⑥ 管理控制中心对所有终端上报的流量速率数据进行实时排名刷新，采取 do-by-need 的方式，在用户请求排名的时候，实时计算最新的流量速率的排名列表。



系统自动升级

■ **目标描述**

在无须运维管理人员参与的情况下，对天擎客户端软件、管理控制台软件、天擎客户端病毒特征库、系统/应用的漏洞补丁进行自动下载、升级与安装。

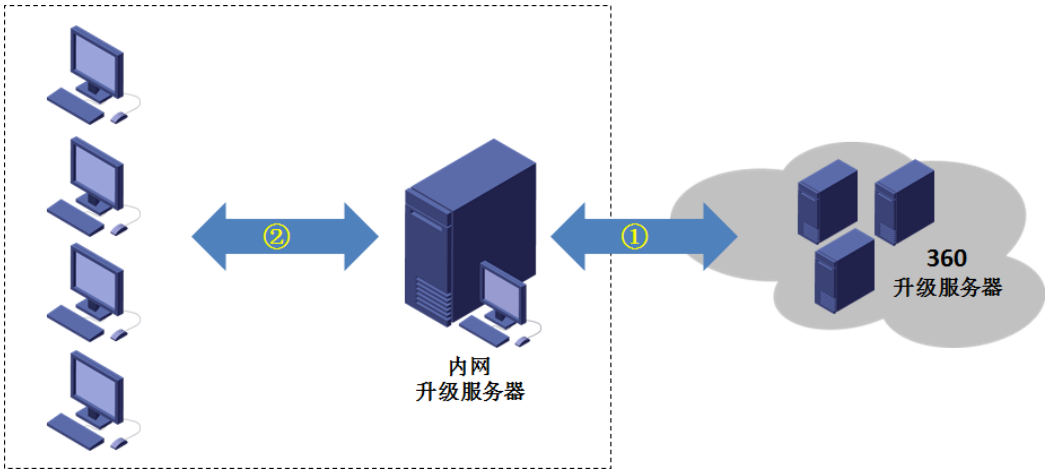
■ **设计描述**

为了避免升级过程中导致网络拥塞，终端的升级将从内网的升级服务器统一拉取升级文件，即终端不会从位于 Internet 的升级服务器下载升级文件。

当天擎管理控制台处于隔离网与非隔离网两种环境之下，其升级方案也有比较大的区别，天擎支持对于隔离网环境下的物理隔离升级与非隔离网环境下的内网推送式升级。

升级过程一共分两个阶段：

- 第一阶段：升级服务器（一般来说就是管理控制台）从位于 Internet 上的升级服务器下载全部升级文件至本地。
- 第二阶段：天擎客户端根据自己的实际需要从升级服务器上下载升级所需要的文件并执行升级操作。



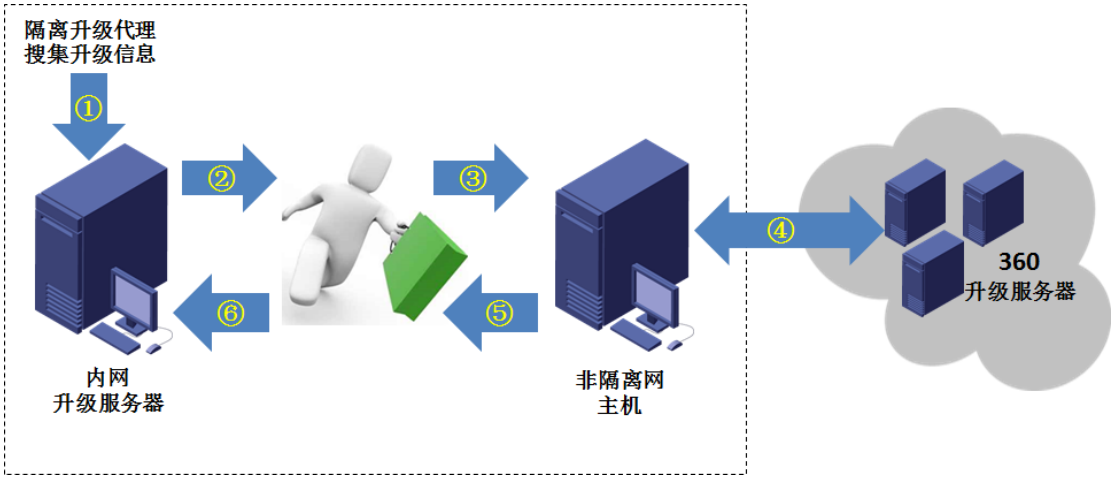
对于隔离网环境来说，由于内网升级服务器无法连接至升级服务器，因此无法直接完成升级文件的下载，在这种情况下，我们提供了“隔离升级代理”工具完成升级文件的下在工作，具体升级过程如下：

第一步：将“隔离升级代理”工具放置在内网升级服务器上，运行该工具，即可完成升级所需信息的收集工作，即搜集到内网服务器中当前升级文件的版本信息，建立升级基线。

第二步：将“隔离升级代理”和所搜集到的升级服务器的升级基线拷贝到一台可以连接至互联网升级服务器的机器上，并再次运行该升级工具，此时，“隔离升级代理”工具将根据当前最新的升级文件与第一步中采集到的升级基线进行对比，下载新增、修改的文件，并将下载到的文件保存在“隔

离升级代理”工具所在的文件夹中。

第三步：再次将“隔离升级代理”文件夹整体拷贝到内网升级服务器之上，再次运行该工具，即可将最新的升级文件成功存放在内网升级服务器上的制定存储位置。



升级过程中的带宽利用

为了最大限度降低升级过程中的带宽消耗，保障业务运行带宽不受升级过程影响，天擎采用如下的技术保证升级过程中的网络稳定性与业务稳定性：

- 带宽压缩技术

  在客户端下载升级文件的过程中，将对升级文件进行压缩处理，尽力降低升级文件传输过程中对带宽的消耗。

- 带宽限制技术

  内网升级服务器支持对升级文件传输的带宽总流量进行限制设置，可以对升级过程中消耗的总带宽进行上限设置。

- 智能分发技术

内网客户端将根据自身的实际需要从内网升级服务器下载不同的特征库升级文件、补丁文件、软件升级包等，而不会将所有的升级文件都从内网升级服务器上下载。

终端硬件性能监控

■ **目标描述**

监控所有终端（包括 VIP 终端）的硬件性能状况，包括：CPU 利用率、内存利用率、硬盘容量与使用情况、网络延迟等。

■ **设计描述**

采样与设值

	采样周期	存储期限	预警阈值
CPU	默认 60 秒，可设置	保存最近 3 个月	可设置
内存	默认 60 秒，可设置	保存最近 3 个月	可设置
硬盘	默认 1 天，可设置	保存最近 3 个月	可设置
网络延时	默认 60 秒，可设置	保存最近 3 个月	可设置

查询与预警

- 支持通过 IP、UserID、采样参数、样本值（大于、小于）结合时间段进行查询，绘制出完整的性能曲线。
- 在采样周期到时的时候，如果性能参数满足报警阈值设置，则立即产生报警，报警数据可以通过邮件进行发送。

终端软件进程与服务管理

■ **目标描述**

监控所有终端的所有进程、服务的运行情况，统计不同进程、服务的出现时间、终止时间、运行持续时间等信息，可以强行启动或强行关闭终端进程。

■ **设计描述**

进程、服务监控

- 进程、服务名称。
- 进程、服务描述。
- 进程、服务启动时间。
- 进程、服务终止时间。

- 进程、服务持续运行时间。
- 该进程、服务是否属于强制启动。

进程、服务启动与关闭

- 远程可以强制启动进程、服务，并将该进程、服务列入后继强制启动策略
- 远程可以远程禁止进程、服务，并将该进程、服务列入后继强制禁止策略
- 可设置进程允许，必须或禁止运行，可以保护进程不被结束掉

终端 Agent 强制安装与运行

- **目标描述**

终端 Agent 一旦安装之后，便强制运行，不允许终止 Agent 进程的运行，并且默认情况下不允许卸载，即不能手工卸载 Agent 程序，也不允许第三方工具对 Agent 程序进行删除，如必须卸载 Agent 软件，必须提供卸载密码。

- **设计描述**

防卸载：天擎终端 Agent 通过在卸载程序 uninstaller.exe 加入了密码验证的逻辑，要求在卸载过程中必须提供管理员密码，如果密码不正确，则卸载程序 uninstaller.exe 将拒绝执行卸载操作。

防终止：天擎终端 Agent 通过截获窗体的 Windows 消息，获得用户发出的终止 Agent 进程的消息，通过改写 OnExit()函数，在其中加入验证逻辑，改变进程退出的标准路径，以此防止 Agent 被非法终止。

终端外设管理

- **目标描述**

对主机所能连接的外部设备进行严格管控，具体来说就是对 USB 接口、光驱、软驱等设备进行准入控制，同时可以对 U 盘实现只读控制，以此实现主机的数据安全。

- **设计描述**

本系统在设备驱动层对外部设备进行可接入控制，实现对外部设备的严格准入控制。

外设类型	控制方式
USB 接口	启用/禁用
光驱	启用/禁用
蓝牙	启用/禁用
智能卡	启用/禁用
手机及平板	启用/禁用
打印机	启用/禁用
USB 有线网卡	启用/禁用
USB 无线网卡及热点	启用/禁用
串口	启用/禁用
并口	启用/禁用
U 盘	禁用/只读/读写

终端小工具

- **目标描述**

为管理员提供灵活易用的终端管理与优化工具，方便管理员快速处理终端问题，提高终端管理的运维效率。

- **设计描述**

集成安全卫士的终端安全管理工具。

企业软件商店	管理员在管理端上传终端所需的办公软件，终端可以点击下载并安装
开机加速	对开机启动项进行管理，优化开机速度
系统垃圾清理	清理系统临时文件缓存与 IE 临时文件缓存
硬件信息查看器	查看硬件物理信息与状态信息
网络查看器	查看网络的状态

终端信息搜集

■ 目标描述

统计终端上的系统信息与软件信息，为管理员管理系统提供详尽的依据，同时根据所搜集到的终端信息生成报表。

■ 设计描述

操作系统	Windows 操作系统的版本、补丁信息
Office	Office 的版本、补丁信息
浏览器	IE 浏览器的版本、补丁信息
防病毒软件	防病毒软件的版本、补丁信息

文件审计管控

■ 目标描述

对终端用户使用文件、打印机、收发邮件等行为进行细粒度的审计和管控。

■ 设计描述

① 文件审计与管控

对指定扩展名文件的读取、修改、删除、移动等行为的审计功能，支持对指定路径或扩展名文件的读取、修改、删除、移动等行为的限制及审计功能，同时，对于终端共享目录的输出、读取及终端用户对网络文件的访问也可进行详细的审计。

② 打印审计与管控

对网络打印机的审计与管控功能，对终端的打印动作、打印文件信息进行审计，也可禁止使用打印机或禁止打印某类文件，可有效防止核心数据通过纸质文件外泄。

③ 邮件审计与管控

对客户端邮件发送审计与管控功能，可禁止客户端发送任何邮件，减少核心数据通过电子邮件外传的风险。

统一运维

软件分发

- **目标描述**

管理控制台可以对指定终端（或终端群组）强制推送软件，被推送的终端无法选择是否接收被推送的软件，同时，被推送的软件到达终端之后，可以选择是否立即安装。

- **设计描述**
  - ✓ 控制端可以选择推动的终端（通过 UserID、IP、网段、IP 区间）。
  - ✓ 推动可以选择定时进行。
  - ✓ 推送过程中压缩传输。
  - ✓ 可以指定推送后的存储位置（存储路径）。
  - ✓ 可以指定推送过程总带宽上限。
  - ✓ 可以指定推送后是否立即安装。

策略下发

- **目标描述**

策略管理的目的是对包括外设、流量、应用等控制对象下发控制策略，具体要求可以按照 UserID、IP、部门、子网、IP 范围、设备分组等进行策略制定。

- **设计描述**

根据项目要求，我们在方案中设计了三维策略控制体系：

- 时间

  在什么时间段内实施控制，即控制生效。

- 对象

  对什么对象实施控制（用户（UserID）、服务器设备（IP）、部门、子网、IP 范围、应用、流量、其他）。

- 控制内容

  对象的控制范围的具体值（应用是否可以按装、终端是否能够准入、流量的具体限流值）。

在策略下发的时候，将根据控制对象进行定点推送，与策略无关的非受控对象不会收到所推动的策略。

在线用户统计

- **目标描述**

统计当前在线、离线的用户数量。提供查询功能，查询指定的用户是否在线，提供查询功能，查询指定的组内在线、离线的用户数量。

- **设计描述**

终端定时打点

① 终端开机之后与管理控制中心进行通信，定时（如：每 30 秒）向管理控制中心执行一次打点操作。

② 管理控制中心为每个终端设置一个定时器，该定时器初始值为 40 秒，如果在定时器到时，但还没收到该终端的打点信息，则管理控制中心主动向该终端发起一次状态探测请求，若该请求 5 秒内无响应，则该终端置为“离线”状态，同时停止该终端定时器；若该请求 5 秒内返回应答，则该终端置为“在线”状态，同时将定时器清零，重新开始计时。

状态统计与查询

③ 统计全网在线与离线终端的数量，同时给出这些终端的 IP、MAC、主机名、对应的用户名、用户所属的部门等。

④ 根据时间、部门、用户名、IP、MAC 查询主机的在线与理想状态，并可导出成 CSV 格式。

安装包定制与 Web 安装

- **目标描述**

为管理员提供定制终端安装包的能力，其中包括：指定终端的管理控制中心IP、指定终端的管理控制中心服务端口等信息，这样，在终端安装的时候，就无需进行额外的交互操作就可以完成安装。

另外，终端可以通过访问 Web 的方式实现一键式安装，无需进行额外的操作即可完成安装操作。

■ 设计描述

配置植入

系统允许管理员可以在管理控制端提供为终端定制安装包的操作，具体来说，就是可以为终端安装包植入如下两方面信息：

- 该终端所需连接的 DNS 服务器信息（包括 IP 地址、端口）。
- 该终端所需连接的管理控制中心的信息（包括 IP 地址、端口）。

这两方面的信息将通过写入装包配置文件的方式植入到终端安装包之中，从而简化终端的配置过程，实现一键式安装。

Web 化安装

为了尽量简化终端的安装过程，提高全网终端的快速部署能力，本系统在方案设计的时候提供了三种 Web 化安装方式。

- DNS 重定向 Web 安装

  这种安装方案需要与 DNS 加壳准入方案相结合，利用 DNS 重定向功能，将未安装 Agent 的终端强制牵引至安装页面进行手工安装操作，在本项目中，可以预计大部分终端将采用此方案。

- 直接访问控制中心 Web 安装页面

  采用这种安装方式，需要事先将控制中心的安装地址采用邮件通知的方式发送给各终端，各终端通过访问控制中心，进入到终端安装页面之中，点击安装按钮进行自动安装。

- IE 控件化安装

采用这种安装方式，需访问安装页面，不同的是无需点击安装按钮，页面自动会弹出安装控件的提示，选择确认即可进入到终端安装程序之中，预计采用这种安

装方式的终端数量不会很多。

系统兼容性

- **目标描述**

  支持多种版本 Windows 操作系统与 B/S 管理架构。

- **设计描述**

  Windows Server 2003（32 位 & 64 位）

  Windows Server 2008（32 位 & 64 位）

  Windows XP

  Vista

  Windows 7（32 位 & 64 位）

  Windows 8（32 位 & 64 位）

  管理架构：B/S

系统可扩展性

- **目标描述**

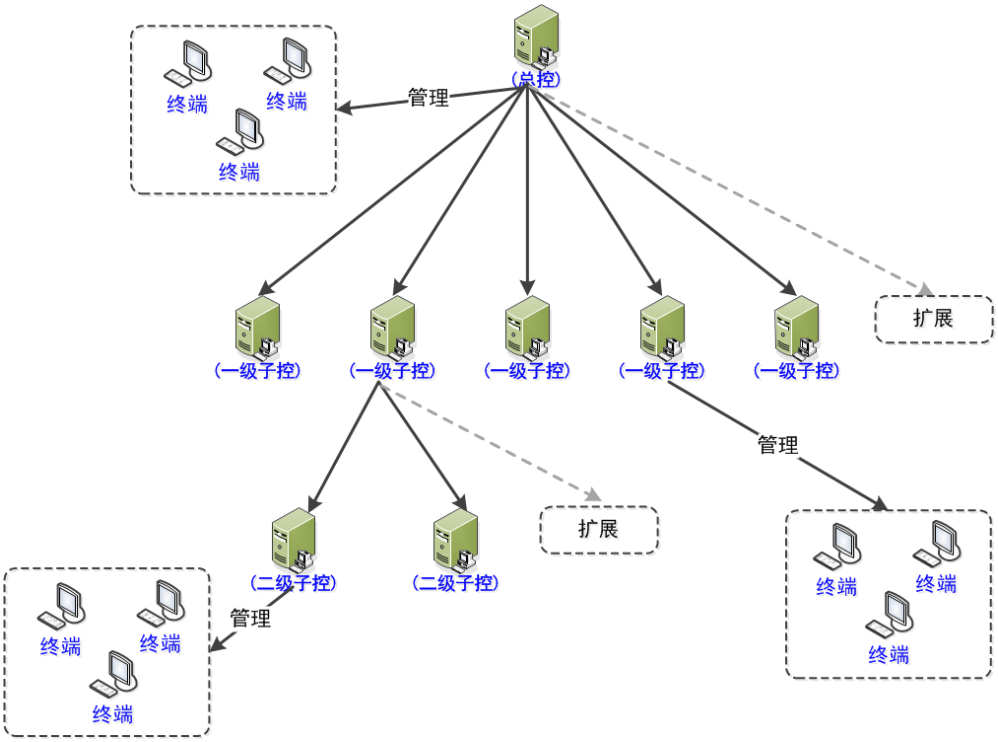
  当前可支撑 6 万终端用户使用，同时在未来发生扩容的情况下，亦可通过增加子控制中心（即分级管理）的方式满足扩容要求。

- **设计描述**

  天擎提供多级管理的功能，通过多级分管，将终端划归到不同的管理控制中心之下，可以实现扩容情况下的灵活扩展方案。

  目前对于标准的服务器（如 DELL 720R，双路 Sand Bridge CPU，单路 8 核，16G 内存，300GB 硬盘）可以有效管理 10000 终端，对于目前 6 万终端来说，可以采用 1 个总控加上 5 个子控，每个控制中心个管理 10000 终端的方式

  未来进行扩容，每增加 10000 终端，相应增加 1 个字控制中心即可满足扩容后的终端管理要求。



系统容灾

■ **目标描述**

在网络瘫痪无法接入网络的情况下终端仍能够正常脱网工作进行正常的病毒查杀。

■ **设计描述**

当网络瘫痪的发生的时候，终端将无法正常连入网络，受此影响，终端也将无法连接升级服务器进行正常的病毒库升级、补丁升级，在这种情况下，终端的防护将面临着新型病毒、新型漏洞利用攻击的危险，为了应对这个问题，天擎中端采用了智能查杀加虚拟补丁的方案，保证在终端无法升级病毒特征库、无法安装补丁文件的情况下，仍然可以对新型病毒、新型威胁进行有效防御：

■ 智能查杀（QVM-II）

智能防护技术（QVM-II）采用人工智能与机器学习的方法，对 20 亿的病毒、木马等恶意代码样本进行学习，提取恶意代码的共性特征，并建立恶意代码的静态行为模型，以此作为对病毒、木马、蠕虫的检测依据，可以在不依赖病毒、木马、恶意代码的个体特征的情况下，实现对病毒、

木马、恶意代码的准确查杀，这种技术保证了在完全没有病毒特征库的情况下也可以高精度地进行检测。

- 虚拟补丁

  主动防御技术采用对文件打开、执行全过程跟踪的方式对系统中加载、打开、运行的文件进行逐步分析，一旦发现有攻击行为，立即加以阻断，这种主动防御技术可以在系统在没有安装补丁的情况下进行主动防御，这种基于主动防御技术的虚拟补丁可以保障终端在没有安装补丁文件的情况下，在受到攻击的时候进行有效防御。