ICS 35.040
L 80

GA

中华人民共和国公共安全行业标准

GA/T 1541—2018

信息安全技术
虚拟化安全防护产品安全技术要求和测试评价方法

Information security technology Security technical requirements and evaluation approaches for virtualization security products

2018－12－27 发布　　2018－12－27 实施

中华人民共和国公安部　发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：国家计算机病毒应急处理中心、公安部十一局七处、天津市公安局网络安全保卫总队、趋势科技（中国）有限公司、北京瑞星信息技术有限公司、卡巴斯基技术开发（北京）有限公司、北京启明星辰信息安全技术有限公司、恒安嘉新（北京）科技股份公司、北京安天网络安全技术有限公司、北京天融信科技有限公司。

本标准主要起草人：陈建民、杜振华、张俊兵、陆磊、曹鹏、张韫菁、刘彦、黄一斌、赵晓明、张鑫、冯军亮、王文一、杨人玮、童宁、刘思宇、冷健波、徐雨晴、崔婷婷、赵焕菊、王龑。

信息安全技术 虚拟化安全防护产品安全技术要求和测试评价方法

1 范围

本标准规定了虚拟化安全防护产品的安全功能要求、性能要求、安全保障要求及等级划分要求。

本标准适用于虚拟化安全防护产品的设计、开发及检测。

2 术语和定义

下列术语和定义适用于本文件。

2.1

虚拟化安全防护产品 virtualization security product

为IT虚拟化环境提供安全防护的产品。除了对病毒、网络攻击等传统的网络安全风险以外，能够针对IT虚拟化带来的新型安全风险进行防护，同时产品运行和产品管理更加适应IT虚拟化环境。

2.2

虚拟化环境 virtualization environment

将计算机资源进行抽象后形成的IT环境，这些资源包括操作系统，计算机系统，CPU，内存，硬盘，负载均衡，路由器等，通过虚拟化出来的计算机资源，用户可以像用未虚拟化访问物理资源的形式，来访问虚拟化后的资源。并且这种抽象后的资源，不会受到物力资源配置、地域、实现等因素的影响。

2.3

安全防护虚拟设备 security virtual appliance

以无代理的透明方式在虚拟机上实施安全策略，包括无代理恶意软件防护，无代理防火墙，无代理的IDS/IPS/Web应用防护以及相关的网络安全策略，无代理的系统完整性监控。

2.4

安全防护客户端 security virtual client

以在虚拟机上安装安全防护客户端的方式实施安全策略，包括恶意软件防护，防火墙，IDS/IPS/Web应用防护以及相关的网络安全策略，系统完整性监控。

2.5

安全防护管理平台 security management platform

用于管理部署于用户虚拟化环境中的安全防护虚拟设备以及安全防护客户端，对安全策略进行统一管理和部署，对所有安全事件进行管理。

2.6

病毒检测 virus detection

在虚拟化安全防护产品进行病毒处理时，对于确定的测试环境，能够准确地报出病毒文件和病毒名

称，并记录检测结果的处理方式。

2.7

隔离 quarantine

在虚拟化安全防护产品进行病毒处理时，为保留病毒样本以及受感染的用户文件，而采取将病毒以及受感染的用户文件存储在一个被称之为“隔离区”的受限制存储空间的处理方式。

2.8

清除还原 virus disinfection

在虚拟化安全防护产品对受到病毒感染的宿主文件进行处理时，采取清除其中的恶意代码或使恶意代码失效，恢复宿主文件原有功能的处理方式。

2.9

病毒样本库 virus sample set

病毒样本文件的集合。

3 缩略语

下列缩略语适用于本文件。

IT：信息技术（Information Technology）

IP：网络互联协议（Internet Protocol）

PDF：便携文件格式（Portable Document Format）

HTML：超文本标记语言（Hypertext Markup Language）

CSV：逗号分隔值文件（Comma-Separated Values）

XML：可扩展标记语言（Extensible Markup Language）

4 虚拟化安全防护产品描述

4.1 功能概述

虚拟化安全防护产品是指一种以病毒防护作为其全部或部分功能的产品，用于检测发现或阻止病毒在虚拟化环境中的传播以及对虚拟主机中的操作系统、应用软件和用户文件的篡改、窃取和破坏等。可以接受授权管理员的统一管理，授权管理员可以通过安全防护管理平台根据虚拟化环境自身以及所承载的应用服务的可用性动态调整统一防护策略。

4.2 工作模式概述

4.2.1 有代理方式

在虚拟主机中安装安全防护客户端，接受安全防护管理平台的统一管理，每个安全防护客户端只能对所在虚拟主机进行防护。

4.2.2 无代理方式

在虚拟化环境中安装安全防护虚拟设备，通过虚拟化环境提供的专门接口，访问虚拟化环境中各虚拟主机的内存、磁盘等并进行安全防护。

4.2.3 混合方式

同时采用有代理和无代理方式的工作模式。

5 技术要求

5.1 总体说明

5.1.1 技术要求分类

将虚拟化安全防护产品技术要求分为功能、性能、安全保障要求三个大类。其中，功能要求是对虚拟化安全防护产品应具备的功能提出具体的要求；性能要求是对虚拟化安全防护产品应达到的性能指标做出规定；安全保障要求则针对虚拟化安全防护产品开发者和虚拟化安全防护产品自身提出具体的要求。

5.1.2 安全等级

按照虚拟化安全防护产品的安全功能要求强度，将虚拟换安全防护产品安全功能要求划分成基本级和增强级；安全保证要求基本级参照了EAL2级安全保证要求，增强级在EAL4级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

增强级产品除需满足基本级产品的技术要求外，还需满足增强级中列出的其他技术要求。其中**“加粗宋体字”**表示所描述的要求仅适用于增强级产品。

5.2 功能要求

5.2.1 基本级

5.2.1.1 防护能力

产品应具备以下防病毒能力：

a) 计算机病毒进入虚拟化环境时发出告警；

b) 不对正常的系统程序文件、应用程序文件、文档、程序代码和数据等产生误报警。

5.2.1.2 防护策略

5.2.1.2.1 策略自定义

产品应能根据要求添加、修改和删除安全策略。

5.2.1.2.2 策略初始模版

产品应具备初始的安全策略，并至少覆盖对病毒文件的检测和清除处理方式。

5.2.1.2.3 统一检测策略

产品应支持对虚拟化环境中统一检测的策略管理，避免统一检测对虚拟化环境可用性造成严重影响。

5.2.1.3 响应处理

产品应能够对检测到的病毒进行处理，处理方式应包括以下种类的一种或多种：

a) 阻止，即产品能够对阻止病毒文件的运行、恶意操作或传播；

b) 删除，即产品能够将病毒文件删除；

c) 隔离，即产品能够将病毒文件从原有位置删除，并备份到一个受限的“隔离区”内。

5.2.1.4 告警信息

产品应能对防病毒等提供告警功能。告警信息应至少包括以下内容：

a) 病毒文件名；
b) 病毒名称；
c) 事件发生的日期和时间；
d) 感染主机信息。

5.2.1.5 安全日志

5.2.1.5.1 事件记录

产品应能对安全防护、策略更改、响应处理、系统升级、安全管理、身份鉴别等安全事件及时生成事件记录，事件记录应存储于掉电非易失性存储介质中，且在存储空间达到阈值时能够通知授权管理员。

5.2.1.5.2 日志导出

日志应能输出成方便阅读的文件格式，至少支持以下文件格式中的一种或多种：TXT、DOC、PDF、HTML、XLS、CSV、XML等。

5.2.1.5.3 日志保存

产品应能够允许用户自定义日志保存期限，但最低保存期限不应少于六个月。

5.2.1.5.4 统计功能

产品应提供基于时间、事件等进行统计的功能。

5.2.1.6 升级能力

5.2.1.6.1 升级更新

对本地特征库及服务程序提供手动及自动的方式进行升级更新。

5.2.1.6.2 推送升级

支持向虚拟化环境推送升级更新。

5.2.1.6.3 升级的有效控制

通过策略对升级进行有效的控制，避免升级对虚拟化环境的应用造成影响。

5.2.1.7 标识与鉴别

5.2.1.7.1 管理员标识

5.2.1.7.1.1 属性定义

产品应为每个授权管理员规定与之相关的安全属性，如标识、鉴别信息、隶属组、权限等。

5.2.1.7.1.2 属性初始化

产品应提供使用默认值对创建的每个授权管理员的属性进行初始化的能力。

5.2.1.7.1.3 唯一性标识

产品应为授权管理员提供唯一标识，并能将标识与该授权管理员的所有可审计事件相关联。

5.2.1.7.2 身份鉴别

5.2.1.7.2.1 基本鉴别

产品应在执行任何与安全功能相关的操作之前鉴别授权管理员的身份，且至少采用一种用户身份鉴别方式。

5.2.1.7.2.2 鉴别数据保护

产品应保证鉴别数据不被未授权查阅或修改。

5.2.1.7.2.3 鉴别失败处理

当对管理员鉴别失败的次数达到指定次数后，产品应能终止管理员的访问。

5.2.1.8 安全管理

5.2.1.8.1 安全功能管理

授权管理员应能对产品进行以下管理操作：

a) 查看、修改相关安全属性；
b) 启动、关闭全部或部分安全功能；
c) 制定和修改各种安全策略。

5.2.1.8.2 安全角色权限分离

产品应能对特权角色和权限进行区分：

a) 具有至少两种不同权限的安全角色，如：管理员和审计员；
b) 产品对特权角色采用最小授权原则，如：管理员不能对审计员负责的审计功能进行管理，审计员也不能对管理员负责的功能进行管理。

5.2.1.8.3 安全管理方式

授权管理员的管理过程应当采取保密措施。

5.2.1.8.4 推送安全策略

安全防护管理平台应提供向客户端推送安全策略和配置更新的功能。

5.2.2 增强级

5.2.2.1 防护能力

5.2.2.1.1 病毒检测

产品应具备以下防病毒能力：

a) 计算机病毒进入虚拟化环境时发出告警；
b) 不对正常的系统程序文件、应用程序文件、文档、程序代码和数据等产生误报警。

5.2.2.1.2 过滤防护

根据策略对网络请求和响应进行阻断过滤。

5.2.2.1.3 攻击防护

产品应具有对以下攻击方式进行防护的能力：

a) 产品能够阻断常见的网络攻击；
b) 产品能够对已知的漏洞进行屏蔽。

5.2.2.2 防护策略

5.2.2.2.1 策略自定义

产品应能根据要求添加、修改和删除安全策略。

5.2.2.2.2 策略初始模版

产品应具备初始的安全策略，并至少覆盖对病毒文件的检测和阻断处理方式。

5.2.2.2.3 统一检测策略

产品应支持对虚拟化环境中统一检测的策略管理，避免统一检测对虚拟化环境可用性造成严重影响。

5.2.2.3 响应处理

产品应能够对检测到的病毒进行处理，处理方式应包括以下种类的一种或多种：

a) 阻止，即产品能够对阻止病毒文件的运行、恶意操作或传播；
b) 删除，即产品能够将病毒文件删除；
c) 隔离，即产品能够将病毒文件从原有位置删除，并备份到一个受限的“隔离区”内；
d) 清除还原，即产品能够对已感染病毒的宿主程序文件或已感染病毒的操作系统中被病毒篡改的系统配置、系统文件等进行修复，使其恢复正常状态。

5.2.2.4 告警信息

产品应能对防病毒、病毒检测、过滤防护、攻击防护等提供告警功能。告警信息应至少包括以下内容：

a) 病毒告警信息：
   1) 病毒文件名；
   2) 病毒名称；
   3) 事件发生的日期和时间；
   4) 感染主机信息。
b) 过滤防护告警：
   1) 网络请求源地址；
   2) 网络请求源端口号；
   3) 网络请求目的地址；
   4) 网络请求目的端口号；
   5) 过滤阻断原因；
   6) 事件发生的日期和时间。
c) 攻击防护告警：
   1) 网络攻击源地址；
   2) 网络攻击源端口号；
   3) 网络攻击目的地址；
   4) 网络攻击目的端口号；
   5) 网络攻击类型；
   6) 事件发生的日期和时间；
   7) 屏蔽漏洞信息；
   8) 漏洞修补信息。

5.2.2.5 告警方式

产品告警应采用屏幕实时提示、邮件告警、短信告警、声音报警等一种或多种方式。

5.2.2.6 即时保护

产品应具备以下即时保护功能：

a) 新的虚拟机开机的时候能够得到即时保护；

b) 虚拟机休眠以后，恢复开机能够得到即时保护，无需更新策略；

c) 虚拟机发生迁移之后，能够自动继承新环境的安全策略。

5.2.2.7 安全日志

5.2.2.7.1 事件记录

产品应能对安全防护、策略更改、响应处理、系统升级、安全管理、身份鉴别等安全事件及时生成事件记录，事件记录应存储于掉电非易失性存储介质中，且在存储空间达到阈值时能够通知授权管理员。

5.2.2.7.2 日志导出

日志应能输出成方便阅读的文件格式，至少支持以下文件格式中的一种或多种：TXT、DOC、PDF、HTML、XLS、CSV、XML等。

5.2.2.7.3 日志保存

产品应能够允许用户自定义日志保存期限，但最低保存期限不应少于六个月。

5.2.2.7.4 统计功能

产品应提供基于时间、事件等进行统计的功能。

5.2.2.8 升级能力

5.2.2.8.1 升级更新

对本地特征库及服务程序提供手动及自动的方式进行升级更新。

5.2.2.8.2 推送升级

支持向虚拟化环境推送升级更新。

5.2.2.8.3 升级的有效控制

通过策略对升级进行有效的控制，避免升级对虚拟化环境的应用造成影响。

5.2.2.9 标识与鉴别

5.2.2.9.1 管理员标识

5.2.2.9.1.1 属性定义

产品应为每个授权管理员规定与之相关的安全属性，如标识、鉴别信息、隶属组、权限等。

5.2.2.9.1.2 属性初始化

产品应提供使用默认值对创建的每个授权管理员的属性进行初始化的能力。

5.2.2.9.1.3 唯一性标识

产品应为授权管理员提供唯一标识，并能将标识与该授权管理员的所有可审计事件相关联。

5.2.2.9.2 身份鉴别

5.2.2.9.2.1 基本鉴别

产品应在执行任何与安全功能相关的操作之前鉴别授权管理员的身份，**并应采用两种或两种以上的用户身份组合鉴别方式。**

5.2.2.9.2.2 鉴别数据保护

产品应保证鉴别数据不被未授权查阅或修改。

5.2.2.9.2.3 鉴别失败处理

当对管理员鉴别失败的次数达到指定次数后，产品应能终止管理员的访问。

5.2.2.10 安全管理

5.2.2.10.1 安全功能管理

授权管理员应能对产品进行以下管理操作：

a) 查看、修改相关安全属性；
b) 启动、关闭全部或部分安全功能；
c) 制定和修改各种安全策略。

5.2.2.10.2 安全角色权限分离

产品应能对管理员角色进行区分：

a) 具有至少两种不同权限的安全角色，如：管理员和审计员；
b) 产品对特权角色采用最小授权原则，如：管理员不能对审计员负责的审计功能进行管理，审计员也不能对管理员负责的功能进行管理。

5.2.2.10.3 安全管理方式

授权管理员的管理过程应当采取保密措施。

5.2.2.10.4 推送安全策略

安全防护管理平台应提供向客户端推送安全策略和配置更新的功能。

5.3 性能要求

5.3.1 基本级

不做要求。

5.3.2 增强级

5.3.2.1 扫描效能

在进行虚拟化环境统一扫描时，整体资源占用不应超过系统资源的20%。

5.3.2.2 资源消耗

在安装部署虚拟化安全产品时，原虚拟环境的可用资源减少不应超过30%。

5.4 安全保障要求

5.4.1 基本级

5.4.1.1 开发

5.4.1.1.1 安全架构描述

开发者应向评估者提供产品安全功能安全架构的描述，安全架构的描述应满足以下要求：

a) 与在产品设计文档中对安全功能要求执行的抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 安全架构的描述论证产品安全功能可防止被破坏；
e) 安全架构的描述论证产品安全功能可防止安全功能要求执行的功能被旁路。

5.4.1.1.2 安全执行功能规范

开发者应向评估者提供一个功能规范，功能规范应满足以下要求：

a) 完整地描述产品安全功能；
b) 描述所有的产品安全功能接口的目的、使用方法以及每个安全功能接口相关的所有参数；
c) 对于每个安全功能要求，功能规范描述执行安全功能接口相关的安全功能执行行为；
d) 对于安全功能要求，功能规范描述由安全功能执行行为相关处理而引起的直接错误信息；
e) 功能规范论证安全功能要求到安全功能接口的对应关系。

5.4.1.1.3 基础设计

开发者应向评估者提供产品的设计文档，并提供从功能规范的产品安全功能接口到产品设计中获取到的最低层分解的映射，应满足以下要求：

a) 设计文档根据子系统描述产品的结构；
b) 设计文档标识产品安全功能的所有子系统；
c) 设计文档对每一个安全功能要求支撑或安全功能要求无关的产品安全功能子系统的行为进行足够详细的描述，以确定它不是安全功能要求执行；
d) 设计文档概括安全功能要求执行子系统的安全功能要求执行行为；
e) 设计文档描述产品安全功能的安全功能要求执行子系统间的相互作用，以及产品安全功能的安全功能要求执行子系统与其它产品安全功能子系统间的相互作用；
f) 映射关系证明产品设计中描述的所有行为能够映射到调用它的产品安全功能接口。

5.4.1.2 指导性文档

5.4.1.2.1 准备程序

开发者应向评估者提供产品的准备程序，满足以下要求：

a) 准备程序描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 准备程序描述安全安装产品以及安全准备与安全目标中描述的运行环境安全目的一致的运行环境必需的所有步骤。

5.4.1.2.2 操作用户指南

开发者应向评估者提供明确和合理的操作用户指南，操作用户指南应满足以下要求：

a) 操作用户指南对每一种用户角色进行描述，在安全处理环境中应被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 操作用户指南对每一种用户角色进行描述，怎样以安全的方式使用产品提供的可用接口；
c) 操作用户指南对每一种用户角色进行描述，可用功能和接口，尤其是受用户控制的所有安全参数，适当时应指明安全值；

d) 操作用户指南对每一种用户角色明确说明，与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变产品安全功能所控制实体的安全特性；
e) 操作用户指南标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），它们与维持安全运行之间的因果关系和联系；
f) 操作用户指南对每一种用户角色进行描述，为了充分实现安全目标中描述的运行环境安全目的所必须执行的安全策略。

5.4.1.3 生命周期支持

5.4.1.3.1 配置管理系统的使用

开发者应向评估者使用配置管理系统，提供配置管理文档，并满足以下要求：
a) 给产品标记唯一参照号；
b) 配置管理文档描述用于唯一标识配置项的方法；
c) 配置管理系统唯一标识所有配置项。

5.4.1.3.2 部分产品配置管理覆盖

开发者应向评估者提供产品配置项列表，满足以下要求：
a) 配置项列表包括：产品本身、安全保障要求的评估证据和产品的组成部分；
b) 配置项列表唯一标识配置项；
c) 对于每一个产品安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

5.4.1.3.3 交付程序

开发者应将把产品或其部分交付给消费者的程序文档化，并满足以下要求：
a) 交付文档应描述在向消费者分发产品版本时，用以维护安全性所必需的所有程序；
b) 确认开发者在使用交付程序。

5.4.1.4 测试

5.4.1.4.1 覆盖证据

开发者应向评估者提供测试覆盖的证据，并满足要求：在测试覆盖证据中，表明测试文档中的测试与功能规范中的安全功能接口是对应的。

5.4.1.4.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档，测试文档应包括以下内容：
a) 测试计划，标识要执行的测试并描述执行每个测试的方案，这些方案包括对于其它测试结果的任何顺序依赖性；
b) 预期的测试结果，指出测试成功执行后的预期输出；
c) 实际的测试结果，确认和预期的测试结果的一致性。

5.4.1.4.3 独立测试—抽样

开发者应向评估者提供一组与开发者产品安全功能测试中同等的一系列资源，用于安全功能的抽样测试。

5.4.1.5 脆弱性分析

开发者应向评估者提供适合测试的产品，并提供执行脆弱性分析的相关资源，包括指导性文档、功能规范、产品设计和安全架构描述。

5.4.2 增强级

5.4.2.1 开发

5.4.2.1.1 安全架构描述

开发者应向评估者提供产品安全功能安全架构的描述，安全架构的描述应满足以下要求：

a) 与在产品设计文档中对安全功能要求执行的抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 安全架构的描述论证产品安全功能可防止被破坏；
e) 安全架构的描述论证产品安全功能可防止安全功能要求执行的功能被旁路。

5.4.2.1.2 完备的功能规范

开发者应向评估者提供一个功能规范，功能规范应满足以下要求：

a) 完整地描述产品安全功能；
b) 描述所有的产品安全功能接口的目的、使用方法以及每个安全功能接口相关的所有参数；
c) **对于每个安全功能要求，功能规范描述执行安全功能接口相关的所有行为；**
d) **功能规范描述可能由每个安全功能接口的调用而引起的所有直接错误消息；**
e) 功能规范论证安全功能要求到安全功能接口的对应关系。

5.4.2.1.3 基础模块设计

开发者应向评估者提供产品的设计文档，并提供从功能规范的产品安全功能接口到产品设计中获取到的最低层分解的映射，应满足以下要求：

a) 设计文档根据子系统描述产品的结构；
b) **设计文档根据模块描述产品安全功能；**
c) **设计文档标识产品安全功能的所有子系统，描述每一个产品安全功能子系统以及产品安全功能所有子系统间的相互作用；**
d) **设计文档提供产品安全功能子系统到产品安全功能模块间的映射关系；**
e) **设计文档描述每一个安全功能要求执行模块，包括它的目的及与其它模块间的相互作用；**
f) **设计文档描述每一个安全功能要求执行模块，包括它的安全功能要求相关接口、其它接口的返回值、与其它模块间的相互作用及调用的接口；**
g) **设计文档描述每一个安全功能要求支撑或安全功能要求无关模块，包括它的的目的及与其它模块间的相互作用；**
h) 映射关系证明产品设计中描述的所有行为能够映射到调用它的产品安全功能接口。

5.4.2.1.4 安全功能实现表示

开发者应以开发人员使用的形式提供实现表示，并向评估者提供产品设计描述与实现表示实例之间的映射，应满足以下要求：

a) **实现表示包含全部产品安全功能；**
b) **实现表示详细地定义安全功能，使得无须进一步设计就能生成安全功能；**
c) **产品设计描述与实现表示示例之间的映射能证明它们的一致性。**

5.4.2.2 指导性文档

5.4.2.2.1 准备程序

开发者应向评估者提供产品的准备程序，满足以下要求：

a) 准备程序描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 准备程序描述安全安装产品以及安全准备与安全目标中描述的运行环境安全目的一致的运行环境必需的所有步骤。

5.4.2.2.2 操作用户指南

开发者应向评估者提供明确和合理的操作用户指南，操作用户指南应满足以下要求：
a) 操作用户指南对每一种用户角色进行描述，在安全处理环境中应被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 操作用户指南对每一种用户角色进行描述，怎样以安全的方式使用产品提供的可用接口；
c) 操作用户指南对每一种用户角色进行描述，可用功能和接口，尤其是受用户控制的所有安全参数，适当时应指明安全值；
d) 操作用户指南对每一种用户角色明确说明，与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变产品安全功能所控制实体的安全特性；
e) 操作用户指南标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），它们与维持安全运行之间的因果关系和联系；
f) 操作用户指南对每一种用户角色进行描述，为了充分实现安全目标中描述的运行环境安全目的所必须执行的安全策略。

5.4.2.3 生命周期支持

5.4.2.3.1 配置管理系统的使用

开发者应向评估者使用配置管理系统，提供配置管理文档，并满足以下要求：
a) 给产品标记唯一参照号；
b) 配置管理文档描述用于唯一标识配置项的方法；
c) 配置管理系统唯一标识所有配置项。

5.4.2.3.2 部分产品配置管理覆盖

开发者应向评估者提供产品配置项列表，满足以下要求：
a) 配置项列表包括：产品本身、安全保障要求的评估证据和产品的组成部分；
b) 配置项列表唯一标识配置项；
c) 对于每一个产品安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

5.4.2.3.3 生产支持和接受程序及其自动化

开发者应使用配置管理系统，提供配置管理文档，并满足以下要求：
a) **给产品标记唯一参照号；**
b) **配置管理文档描述用于唯一标识配置项的方法；**
c) **配置管理系统唯一标识所有配置项；**
d) **配置管理系统提供自动化的措施使得只能对配置项进行授权变更；**
e) **配置管理系统以自动化的方式支持产品的生产；**
f) **配置管理文档包括配置管理计划，配置管理计划应描述配置管理系统是如何应用于产品的开发的；**
g) **配置管理计划描述用来接受修改过的或新创建的作为产品组成部分的配置项的程序；**
h) **提供证据论证所有配置项都正在配置管理系统下进行维护，并论证配置管理系统的运行与配置管理计划是一致的。**

5.4.2.3.4 问题跟踪配置管理覆盖

开发者应向评估者提供产品配置项列表，满足以下要求：

a) **配置项列表包括：产品本身、安全保障要求的评估证据、产品的组成部分、实现表示和安全缺陷报告及其解决状态；**

b) **配置项列表唯一标识配置项；**

c) **对于每一个产品安全功能相关的配置项，配置项列表简要说明该配置项的开发者。**

5.4.2.3.5 交付程序

开发者应将把产品或其部分交付给消费者的程序文档化，并满足以下要求：

a) 交付文档描述，在向消费者分发产品版本时，用以维护安全性所必需的所有程序；

b) 确认开发者在使用交付程序。

5.4.2.3.6 安全措施标识

开发者应向评估者提供开发安全文档，满足以下要求：

a) **开发安全文档描述在产品的开发环境中，保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的及其它方面的安全措施；**

b) **确认安全措施在被使用。**

5.4.2.3.7 开发者定义的生命周期模型

开发者应建立一个生命周期模型用于产品的开发和维护，提供生命周期定义文档，并满足以下要求：

a) **生命周期定义文档对用于开发和维护产品的模型进行描述；**

b) **生命周期模型为产品的开发和维护提供必要的控制。**

5.4.2.3.8 明确定义的开发工具

开发者应标识和明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义所有语句和实现用到的所有协定与命令，以及所有实现依赖选项的含义。

5.4.2.4 测试

5.4.2.4.1 覆盖分析

开发者应向评估者提供测试覆盖分析，并满足如下要求：

a) 测试覆盖分析论证测试文档中的测试与功能规范中的安全功能接口之间的对应性；

b) **测试覆盖分析论证已经对功能规范中的所有产品安全功能接口都进行了测试。**

5.4.2.4.2 测试：安全执行模块

开发者应向评估者提供测试深度分析，并满足以下要求：

a) **测试深度分析论证测试文档中的测试与产品设计中的产品安全功能子系统、安全功能要求执行模块之间的一致性；**

b) **测试深度分析论证产品设计中的所有产品安全功能子系统都已经进行过测试；**

c) **测试深度分析论证产品设计中的安全功能要求执行模块都已经进行过测试。**

5.4.2.4.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档，测试文档应包括以下内容：

a) 测试计划，标识要执行的测试并描述执行每个测试的方案，这些方案应包括对于其它测试结果的任何顺序依赖性；

b) 预期的测试结果，指出测试成功执行后的预期输出；

c） 实际的测试结果，确认和预期的测试结果的一致性。

5.4.2.4.4 独立测试—抽样

开发者应向评估者提供一组与开发者产品安全功能测试中同等的一系列资源，用于安全功能的抽样测试。

5.4.2.5 关注点脆弱性分析

开发者应提供适合测试的产品，并向评估者提供执行关注点脆弱性分析的相关资源，包括指导性文档、功能规范、产品设计、安全架构描述和实现表示。

6 测试评价方法

6.1 总体说明

测评方法与技术要求一一对应，它给出具体的测评方法来验证虚拟化安全防护产品产品是否达到技术要求中所提出的要求。它由测试方法和预期结果四个部分构成。测试中涉及的测试样本库有关说明参见附录 A。

6.2 功能测试

6.2.1 基本级

6.2.1.1 防护能力

该项测试遵循以下测试方法：

a） 测试方法：

1） 启用产品的病毒实时监控策略配置；

2） 通过存储介质、网络等方式向虚拟化环境传送病毒样本库和误报样本库中的文件；

3） 检查虚拟化环境中是否对病毒的传播、破坏进行告警。

b） 预期结果：

1） 在虚拟化环境中应能出现病毒告警提示；

2） 产品对病毒样本基本库至少能检测其中的 90%，对病毒样本流行库至少能检测其中的 95%；

3） 产品不会对误报样本库中的样本进行检测。

6.2.1.2 防护策略

6.2.1.2.1 策略自定义

该项测试遵循以下测试方法：

a） 测试方法：

1） 根据功能要求添加病毒检测过滤策略；

2） 进行检测病毒测试；

3） 根据功能要求修改刚添加的病毒检测过滤策略；

4） 进行检测病毒测试；

5） 根据功能要求删除刚修改的病毒检测过滤策略；

6） 进行检测病毒测试。

b） 预期结果：虚拟化安全防护产品能够根据自定义的策略完成相应的病毒检测。

6.2.1.2.2 策略初始模版

该项测试遵循以下测试方法：

a) 测试方法

1) 检查产品的初始策略模版；

2) 进行检测病毒测试；

3) 检查产品是否按照初始策略模版进行了相应的处理。

b) 预期结果：产品具备基本的过滤防护、攻击防护、病毒阻断的能力。

6.2.1.2.3 统一检测策略

该项测试遵循以下测试方法：

a) 测试方法

1) 在虚拟化环境中使用相应的策略执行统一检测；

2) 检查虚拟化环境的统一检测是否按照策略执行。

b) 预期结果：产品的统一检测功能能够按照策略配置执行，不会虚拟化环境的可用性造成严重影响。

6.2.1.3 响应处理

该项测试遵循以下测试方法：

a) 测试方法如下：

1) 将产品对检测到病毒后的处理策略分别设定为阻止、删除和隔离；

2) 对产品进行病毒检测测试。

b) 预期结果：产品能够按照相应处理策略对病毒进行响应处理。

6.2.1.4 告警信息

该项测试遵循以下测试方法：

a) 测试方法如下：

1) 进行病毒检测测试；

2) 查看产品的告警信息。

b) 预期结果如下：

1) 产品具备告警功能；

2) 产品的告警信息符合 5.2.1.4 中的要求。

6.2.1.5 安全日志

6.2.1.5.1 事件记录

该项测试遵循以下测试方法：

a) 测试方法

1) 配置虚拟化安全防护产品，开启安全日志事件记录功能；

2) 进行各项功能测试；

3) 查看相关的安全事件日志；

4) 检查事件日志存储空间配置，并配置存储空间报警阈值。

b) 预期结果

1) 产品具有安全事件记录日志，并能够完整记录各种安全事件的详细信息；

2) 安全事件存储空间达到报警阈值时，能够通知授权管理员。

6.2.1.5.2 日志导出

该项测试遵循以下测试方法：

a) 测试方法

1) 将安全日志导出为 TXT、DOC、PDF、HTML、XLS、CSV、XML 格式中一种；

2) 检查导出的日志是否能够正常方便打开；

3) 检查导出的日志信息是否完整。

b) 预期结果：导出的日志可方便的阅读，信息完整。

6.2.1.5.3 日志保存

该项测试遵循以下测试方法：

a) 测试方法如下：

1) 查看产品是否能够允许用户自定义日志保存期限；

2) 查看产品允许用户自定义的最低保存期限是否不少于六个月。

b) 预期结果：产品能够允许用户自定义日志保存期限，最低保存期限不少于六个月。

6.2.1.5.4 统计功能

该项测试遵循以下测试方法：

a) 测试方法

1) 将日志的按照于时间、事件等提供的方式进行统计查询；

2) 检查统计的信息是否合理、完整。

b) 预期结果：日志统计正常显示，信息合理完整。

6.2.1.6 升级能力

6.2.1.6.1 升级更新

该项测试遵循以下测试方法：

a) 测试方法

1) 使用手动或自动的方式进行特征库和服务程序的升级更新；

2) 检查特征库和服务程序的版本信息。

b) 预期结果：特征库和服务程序正常更新到最新版本。

6.2.1.6.2 推送升级

该项测试遵循以下测试方法：

a) 测试方法

1) 将升级信息推送至虚拟化环境中；

2) 检查虚拟化环境中产品的版本信息。

b) 预期结果：虚拟终端安全防护产品的版本正常升级到最新版本。

6.2.1.6.3 升级的有效控制

该项测试遵循以下测试方法：

a) 测试方法

1) 启动虚拟化环境特征库升级策略；

2) 启动虚拟化环境安全策略更新；

3) 检查虚拟化环境中是否产生网络风暴等状况。

b) 预期结果：对升级进行了有效的控制，虚拟化环境未受到升级的影响。

6.2.1.7 标识与鉴别

6.2.1.7.1 管理员标识

该项测试遵循以下测试方法：

a) 测试方法

1) 检查虚拟化安全防护产品的授权管理员管理功能，是否有分组、权限分配功能；
2) 按虚拟化安全防护产品提供的默认安全属性创建一个授权管理员；
3) 检查授权管理员标识是否唯一。

b) 预期结果

1) 虚拟化安全防护产品具有较为完整的授权管理员管理功能，具有用户分组、权限分配功能；
2) 虚拟化安全防护产品可以创建一个具有默认安全属性的授权管理员；
3) 授权管理员标识为唯一。

6.2.1.7.2 身份鉴别

该项测试遵循以下测试方法：

a) 测试方法

1) 检查防虚拟化安全防护产品是否有身份鉴别功能；
2) 使用虚拟化安全防护产品相关安全功能前管理员是否需要输入凭据；
3) 检查虚拟化安全防护产品的身份鉴别数据是否能够由未经授权的管理员查阅或修改；
4) 多次尝试输入错误的鉴别凭据，产品能否提示并终止管理员的访问。

b) 预期结果

1) 虚拟化安全防护产品具有管理员身份鉴别功能；
2) 管理员必须输入合法凭据才能使用虚拟化安全防护产品的相关安全功能；
3) 虚拟化安全防护产品的用户身份鉴别数据不会被未经授权的管理员查阅或修改；
4) 多次错误的鉴别凭据将导致管理员被终止访问虚拟化安全防护产品。

6.2.1.8 安全管理

6.2.1.8.1 安全功能管理

该项测试遵循以下测试方法：

a) 测试方法

1) 使用授权管理员的合法凭据登录虚拟换安全防护产品；
2) 查看、修改虚拟化安全防护产品的相关安全属性；
3) 启动、关闭虚拟化安全防护产品的全部或部分安全功能；
4) 新增、修改防虚拟化安全防护产品的病毒处理策略、阻断过滤策略等各种安全策略。

b) 预期结果

1) 授权管理员能够查看、修改相关安全属性；
2) 授权管理员能够启动、关闭虚拟化安全防护产品的全部或部分安全功能；
3) 授权管理员能够新增、修改虚拟化安全防护产品的病毒处理策略、阻断过滤策略等各种安全策略。

6.2.1.8.2 安全角色权限分离

该项测试遵循以下测试方法：

a) 测试方法

1) 检查虚拟化安全防护产品是否有至少两种不同权限的管理员角色；
2) 检查虚拟化安全防护产品是否能够根据不同的功能模块定义不同的权限角色；
3) 为授权管理员分配相应的权限角色；

4) 检查授权管理员是否具有与其角色相符的权限。

b) 预期结果

1) 虚拟化安全防护产品具有至少两种不同权限的授权管理员角色；

2) 虚拟化安全防护产品能够根据不同的功能模块定义不同的权限角色；

3) 角色分配后，授权管理员具有与其角色相符的权限。

6.2.1.8.3 安全管理方式

该项测试遵循以下测试方法：

a) 测试方法

1) 授权管理管理员在虚拟化环境中进行安全管理操作；

2) 检查管理的过程是否进行了加密。

b) 预期结果：授权管理员的管理过程采取保密措施。

6.2.1.8.4 推送安全策略

该项测试遵循以下测试方法：

a) 测试方法

1) 授权管理员在管理中心修改安全策略；

2) 将修改后的安全策略推送到虚拟化环境中；

3) 检查虚拟化环境中的安全策略是否与授权管理员的修改一致。

b) 预期结果：虚拟化环境中安全策略的修改与授权管理员在管理中心进行的修改一致。

6.2.2 增强级

6.2.2.1 防护能力

6.2.2.1.1 病毒检测

该项测试遵循以下测试方法：

a) 测试方法

1) 启用产品的病毒实时监控策略配置；

2) 通过存储介质、网络等方式向虚拟化环境传送病毒样本库和误报样本库中的文件；

3) 检查虚拟化环境中是否对病毒的传播、破坏进行告警。

b) 预期结果

1) 在虚拟化环境中应能出现病毒告警提示；

2) 产品对病毒样本基本库至少能检测其中的 95%，对病毒样本流行库至少能检测其中的 98%；

3) 产品不会对误报样本库中的样本进行检测。

6.2.2.1.2 过滤防护

该项测试遵循以下测试方法：

a) 测试方法

1) 配置基于源 IP 地址、目的 IP 地址的过滤策略，产生相应的网络会话；

2) 配置基于源端口、目的端口的过滤策略，产生相应的网络会话；

3) 配置基于协议类型的过滤策略，产生相应的网络会话；

4) 配置基于文件类型的过滤策略，产生相应的网络会话；

5) 配置用户自定义的过滤策略，过滤条件是 2）～ 5）过滤条件的部分或全部组合，产生相应的网络会话。

b) 预期结果

1） **虚拟化安全防护产品能够根据源 IP 地址、目的 IP 地址进行过滤；**
2） **虚拟化安全防护产品能够根据源端口、目的端口进行过滤；**
3） **虚拟化安全防护产品能够根据协议类型进行过滤；**
4） **虚拟化安全防护产品能够根据文件类型进行过滤；**
5） **虚拟化安全防护产品能够根据用户自定义的策略进行过滤。**

6.2.2.1.3 攻击防护

该项测试遵循以下测试方法：

a） **测评方法**
1） **检查产品的缺省安全策略；**
2） **使用常用的网络攻击用例对虚拟化环境发起攻击；**
3） **利用已知漏洞对虚拟化环境中的应用发起漏洞攻击；**
4） **检查是否阻断了网络攻击行为，并进行了告警。**

b） **预期结果**
1） **常见攻击行为可以被阻断；**
2） **利用已知漏洞的攻击行为可以被阻断。**

6.2.2.2 防护策略

6.2.2.2.1 策略自定义

该项测试遵循以下测试方法：

a） 测试方法
1） 根据功能要求添加病毒检测过滤策略；
2） 进行检测病毒测试；
3） 根据功能要求修改刚添加的病毒检测过滤策略；
4） 进行检测病毒测试；
5） 根据功能要求删除刚修改的病毒检测过滤策略；
6） 进行检测病毒测试；

b） 预期结果：虚拟化安全防护产品能够根据自定义的策略完成相应的病毒检测。

6.2.2.2.2 策略初始模版

该项测试遵循以下测试方法：

a） 测试方法
1） 检查产品的初始策略模版；
2） 进行检测病毒测试；
3） 检查产品是否按照初始策略模版进行了相应的处理。

b） 预期结果：产品具备基本的过滤防护、攻击防护、病毒阻断的能力。

6.2.2.2.3 统一检测策略

该项测试遵循以下测试方法：

a） 测试方法
1） 在虚拟化环境中使用相应的策略执行统一检测；
2） 检查虚拟化环境的统一检测是否按照策略执行。

b） 预期结果：产品的统一检测功能能够按照策略配置执行，不会虚拟化环境的可用性造成严重影响。

6.2.2.3 响应处理

该项测试遵循以下测试方法：

a) 测试方法如下：

1) 按照 5.2.2.3 中列举的方式配置产品的病毒处理方式；

2) 分别进行病毒处理测试；

b) 预期结果：产品能够按照自定义的策略对病毒进行相应处理。

6.2.2.4 告警信息

该项测试遵循以下测试方法：

a) 测试方法如下：

1) 进行病毒检测测试；

2) 查看产品的告警信息。

b) 预期结果如下：

1) 产品具备告警功能；

2) 产品的告警信息符合 5.2.2.4 中的要求。

6.2.2.5 告警方式

该项测试遵循以下测试方法：

a) 测试方法

1) 配置产品的告警方式；

2) 进行各项功能测试；

3) 检查各种告警方式是否有效。

b) 预期结果：支持的告警方式正常提示。

6.2.2.6 即时保护

该项测试遵循以下测试方法：

a) 测试方法

1) 在虚拟化环境中新建虚拟机并启动，向新建虚拟机中拷贝病毒样本；

2) 激活休眠的虚拟机，向被激活的虚拟机中拷贝病毒样本；

3) 在虚拟化环境中迁移虚拟机，向迁移后的虚拟机中拷贝病毒样本；

4) 检查虚拟化环境中是否有告警提示。

b) 预期结果：检查虚拟化环境中是否出现告警提示，是否阻断了病毒文件的传播。

6.2.2.7 安全日志

6.2.2.7.1 事件记录

该项测试遵循以下测试方法：

a) 测试方法

1) 配置虚拟化安全防护产品，开启安全日志事件记录功能；

2) 进行各项功能测试；

3) 查看相关的安全事件日志；

4) 检查事件日志存储空间配置，并配置存储空间报警阈值。

b) 预期结果

1) 产品具有安全事件记录日志，并能够完整记录各种安全事件的详细信息；

2) 安全事件存储空间达到报警阈值时，能够通知授权管理员。

6.2.2.7.2 日志导出

该项测试遵循以下测试方法：

a) 测试方法

1) 将安全日志导出为 TXT、DOC、PDF、HTML、XLS、CSV、XML 格式中一种；

2) 检查导出的日志是否能够正常方便打开；

3) 检查导出的日志信息是否完整。

b) 预期结果：导出的日志可方便的阅读，信息完整。

6.2.2.7.3 日志保存

该项测试遵循以下测试方法：

a) 测试方法如下：

1) 查看产品是否能够允许用户自定义日志保存期限；

2) 查看产品允许用户自定义的最低保存期限是否不少于六个月。

b) 预期结果：产品能够允许用户自定义日志保存期限，最低保存期限不少于六个月。

6.2.2.7.4 统计功能

该项测试遵循以下测试方法：

a) 测试方法

1) 将日志的按照于时间、事件等提供的方式进行统计查询；

2) 检查统计的信息是否合理、完整。

b) 预期结果：日志统计正常显示，信息合理完整。

6.2.2.8 升级能力

6.2.2.8.1 升级更新

该项测试遵循以下测试方法：

a) 测试方法

1) 使用手动或自动的方式进行特征库和服务程序的升级更新；

2) 检查特征库和服务程序的版本信息。

b) 预期结果：特征库和服务程序正常更新到最新版本。

6.2.2.8.2 推送升级

该项测试遵循以下测试方法：

a) 测试方法

1) 将升级信息推送至虚拟化环境中；

2) 检查虚拟化环境中产品的版本信息。

b) 预期结果：虚拟终端安全防护产品的版本正常升级到最新版本。

6.2.2.8.3 升级的有效控制

该项测试遵循以下测试方法：

a) 测试方法

1) 启动虚拟化环境特征库升级策略；

2) 启动虚拟化环境安全策略更新；

3) 检查虚拟化环境中是否产生网络风暴等状况。

b) 预期结果：对升级进行了有效的控制，虚拟化环境未受到升级的影响。

6.2.2.9 标识与鉴别

6.2.2.9.1 管理员标识

该项测试遵循以下测试方法：

a) 测试方法

1) 检查虚拟化安全防护产品的授权管理员管理功能，是否有分组、权限分配功能；
2) 按虚拟化安全防护产品提供的默认安全属性创建一个授权管理员；
3) 检查授权管理员标识是否唯一。

b) 预期结果

1) 虚拟化安全防护产品具有较为完整的授权管理员管理功能，具有用户分组、权限分配功能；
2) 虚拟化安全防护产品可以创建一个具有默认安全属性的授权管理员；
3) 授权管理员标识为唯一。

6.2.2.9.2 身份鉴别

该项测试遵循以下测试方法：

a) 测试方法

1) 检查虚拟化安全防护产品是否有身份鉴别功能；
2) 使用虚拟化安全防护产品相关安全功能前管理员是否需要输入凭据；
3) 检查虚拟化安全防护产品的身份鉴别数据是否能够由未经授权的管理员查阅或修改；
4) 多次尝试输入错误的鉴别凭据，产品能否提示并终止管理员的访问；
5) 检查虚拟化安全防护产品是否对同一管理员采用两种或两种以上组合的用户身份鉴别方式；
6) 多次尝试输入错误的鉴别凭据，产品能否提示并终止管理员的访问。

b) 预期结果

1) 虚拟化安全防护产品具有管理员身份鉴别功能；
2) 管理员必须输入合法凭据才能使用虚拟化安全防护产品的相关安全功能；
3) 虚拟化安全防护产品的用户身份鉴别数据不会被未经授权的管理员查阅或修改；
4) 多次错误的鉴别凭据将导致用户被终止访问虚拟化安全防护产品；
5) 虚拟化安全防护产品对同一用户采用了两种或两种以上组合的用户身份鉴别方式；
6) 多次错误的鉴别凭据将导致管理员被终止访问虚拟化安全防护产品。

6.2.2.10 安全管理

6.2.2.10.1 安全功能管理

该项测试遵循以下测试方法：

a) 测试方法

1) 使用授权管理员的合法凭据登录虚拟化安全防护产品；
2) 查看、修改虚拟化安全防护产品的相关安全属性；
3) 启动、关闭虚拟化安全防护产品的全部或部分安全功能；
4) 新增、修改防虚拟化安全防护产品的病毒处理策略、阻断过滤策略等各种安全策略。

b) 预期结果

1) 授权管理员能够查看、修改相关安全属性；
2) 授权管理员能够启动、关闭虚拟化安全防护产品的全部或部分安全功能；
3) 授权管理员能够新增、修改虚拟化安全防护产品的病毒处理策略、阻断过滤策略等各种安全策略。

6.2.2.10.2 安全角色权限分离

该项测试遵循以下测试方法：

a) 测试方法
   1) 检查虚拟化安全防护产品是否有至少两种不同权限的管理员角色；
   2) 检查虚拟化安全防护产品是否能够根据不同的功能模块定义不同的权限角色；
   3) 为授权管理员分配相应的权限角色；
   4) 检查授权管理员是否具有与其角色相符的权限。
b) 预期结果
   1) 虚拟化安全防护产品具有至少两种不同权限的授权管理员角色；
   2) 虚拟化安全防护产品能够根据不同的功能模块定义不同的权限角色；
   3) 角色分配后，授权管理员具有与其角色相符的权限。

6.2.2.10.3 安全管理方式

该项测试遵循以下测试方法：

a) 测试方法
   1) 授权管理管理员在虚拟化环境中进行安全管理操作；
   2) 检查管理的过程是否进行了加密。
b) 预期结果：授权管理员的管理过程采取保密措施。

6.2.2.10.4 推送安全策略

该项测试遵循以下测试方法：

a) 测试方法
   1) 授权管理员在管理中心修改安全策略；
   2) 将修改后的安全策略推送到虚拟化环境中；
   3) 检查虚拟化环境中的安全策略是否与管理员的修改一致。
b) 预期结果：虚拟化环境中安全策略的修改与管理员在管理中心进行的修改一致。

6.3 性能测试

6.3.1 基本级

无

6.3.2 增强级

6.3.2.1 扫描性能

该项测试遵循以下测试方法：

a) 测试方法
   1) 对虚拟化环境中所有的虚拟机发起统一的全盘扫描；
   2) 记录扫描过程中，虚拟化环境的性能指标；
   3) 检查扫描过程中的资源占用是否超过系统资源的 20%。
b) 预期结果：进行虚拟化环境统一扫描时，整体资源占用不超过系统资源的 20%。

6.3.2.2 资源消耗

该项测试遵循以下测试方法：

a) 测试方法
   1) 检测在部署虚拟化安全防护产品前虚拟化环境的可用资源；
   2) 检测在部署虚拟化安全防护产品后虚拟化环境的可用资源；
   3) 检查部署虚拟化安全防护产品后虚拟化环境的可用资源较少量。

b） **预期结果：在安装部署虚拟化安全防护产品后，虚拟环境的可用资源减少不超过 30%。**

6.4 安全保障评估

6.4.1 基本级

6.4.1.1 开发

6.4.1.1.1 安全架构描述

该项评估应遵循以下评估方法：

a） 评估方法，评估者审查产品安全功能安全架构描述文档，确认是否满足 5.4.1.1.1 中的要求；

b） 预期结果：产品安全功能安全架构描述文档符合 5.4.1.1.1 中的要求。

6.4.1.1.2 安全执行功能规范

该项评估应遵循以下评估方法：

a） 评估方法，评估者审查开发者提供的功能规范文档，确认是否满足 5.4.1.1.2 中的要求；

b） 预期结果：开发者提供了功能规范文档，并且文档符合 5.4.1.1.2 中的要求。

6.4.1.1.3 基础设计

该项评估应遵循以下评估方法：

a） 评估方法如下：

1） 评估者审查开发者提供的产品设计文档，确认是否满足 5.4.1.1.3 中对设计文档的要求；

2） 评估者审查映射关系说明，确认是否满足 5.4.1.1.3 中对映射关系的要求；

3） 评估者确认设计是否所有安全功能要求的正确且完备的实例。

b） 预期结果如下：

1） 开发者提供的产品设计文档，满足基础设计 5.4.1.1.3 中对设计文档的要求；

2） 映射关系说明满足基础设计 5.4.1.1.3 中对映射关系的要求；

3） 能够确认设计是所有安全功能要求的正确且完备的实例。

6.4.1.2 指导性文档

6.4.1.2.1 准备程序

该项评估应遵循以下评估方法：

a） 评估方法如下：

1） 评估者审查开发者提供的准备程序，确认是否满足准备程序 5.4.1.2.1 的要求；

2） 评估者运用准备程序确认产品运行是否能被安全的准备。

b） 预期结果如下：

1） 开发者提供的准备程序，满足准备程序 5.4.1.2.1 的要求；

2） 运用准备程序能够做好产品安全运行的准备。

6.4.1.2.2 操作用户指南

该项评估应遵循以下评估方法：

a） 评估方法，评估者审查开发者提供的操作用户指南，确认是否满足 5.4.1.2.2 的要求；

b） 预期结果：开发者提供的操作用户指南，满足 5.4.1.2.2 的要求。

6.4.1.3 生命周期支持

6.4.1.3.1 配置管理系统的使用

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者审查确认开发者是否使用了配置管理系统；

2） 评估者审查开发者提供的配置管理文档，确认是否满足 5.4.1.3.1 的要求。

b) 预期结果如下：

1） 能够确认开发者使用了配置管理系统；

2） 开发者提供的配置管理文档，满足 5.4.1.3.1 的要求。

6.4.1.3.2 部分产品配置管理覆盖

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的产品配置项列表，确认是否满足 5.4.1.3.2 的要求；

b) 预期结果：开发者提供的产品配置项列表，满足 5.4.1.3.2 的要求。

6.4.1.3.3 交付程序

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者审查开发者提供的交付程序文档，确认是否满足 5.4.1.3.3 的要求；

2） 评估者审查确认开发者是否使用了交付程序。

b) 预期结果如下：

1） 开发者提供的交付程序文档，满足交付程序 5.4.1.3.3 的要求；

2） 能够确认开发者使用了交付程序。

6.4.1.4 测试

6.4.1.4.1 覆盖证据

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的测试覆盖证据，确认是否满足 5.4.1.4.1 的要求；

b) 预期结果：开发者提供的测试覆盖证据，满足覆盖证据 5.4.1.4.1 的要求。

6.4.1.4.2 功能测试

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的功能测试文档，确认是否满足 5.4.1.4.2 的要求；

b) 预期结果：开发者提供的功能测试文档，满足功能测试 5.4.1.4.2 的要求。

6.4.1.4.3 独立测试—抽样

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者执行测试文档中的测试样本，以验证开发者的测试结果是否正确；

2） 评估者测试产品安全功能的一个子集，以确认产品安全功能是否按照规定运行。

b) 预期结果如下：

1） 执行测试文档中的测试样本，验证了开发者的测试结果是正确的；

2） 确认产品安全功能是按照规定运行。

6.4.1.5 脆弱性分析

该项评估应遵循以下评估方法：

a) 评估方法如下：
   1） 评估者执行公共领域的调查以标识产品的潜在脆弱性；
   2） 评估者执行独立的产品脆弱性分析去标识产品潜在的脆弱性，在分析过程中使用开发者提供的指导性文档、功能规范、产品设计和安全架构描述；
   3） 评估者基于已标识的潜在脆弱性实施穿透性测试，确认产品是否能够抵抗具有基本攻击潜力的攻击者的攻击。
b) 预期结果如下：
   1） 开发者提供了适合测试的产品，并提供执行脆弱性分析的相关资源；
   2） 通过脆弱性分析确认产品能够抵抗具有基本攻击潜力的攻击者的攻击。

6.4.2 增强级

6.4.2.1 开发

6.4.2.1.1 安全架构描述

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查产品安全功能安全架构描述文档，确认是否满足 5.4.2.1.1 的要求；
b) 预期结果：产品安全功能安全架构描述文档符合 5.4.2.1.1 的要求。

6.4.2.1.2 完备的功能规范

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的功能规范文档，确认是否满足 5.4.2.1.2 的要求；
b) 预期结果：开发者提供了功能规范文档，并且文档符合 5.4.2.1.2 的要求。

6.4.2.1.3 基础模块设计

该项评估应遵循以下评估方法：

a) 评估方法如下：
   1） 评估者审查开发者提供的产品设计文档，确认是否满足 5.4.2.1.3 中对设计文档的要求；
   2） 评估者审查映射关系说明，确认是否满足 5.4.2.1.3 中对映射关系的要求；
   3） 评估者确认设计是否所有安全功能要求的正确且完备的实例。
b) 预期结果如下：
   1） 开发者提供的产品设计文档，满足 5.4.2.1.3 中对设计文档的要求；
   2） 映射关系说明满足 5.4.2.1.3 中对映射关系的要求；
   3） 能够确认设计是所有安全功能要求的正确且完备的实例。

6.4.2.1.4 安全功能实现表示

该项评估应遵循以下评估方法：

a) 评估方法如下：
   1） 评估者审查开发者提供的实现表示，确认是否满足 5.4.2.1.4 中对实现表示文档的要求；
   2） 评估者审查映射关系说明，确认是否满足 5.4.2.1.4 中对映射关系的要求。
b) 预期结果如下：
   1） 开发者提供的实现表示，满足 5.4.2.1.4 中对实现表示文档的要求；
   2） 映射关系说明满足 5.4.2.1.4 中对映射关系的要求。

6.4.2.2 指导性文档

6.4.2.2.1 准备程序

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者审查开发者提供的准备程序，确认是否满足 5.4.2.2.1 的要求；

2） 评估者运用准备程序确认产品运行是否能被安全的准备。

b) 预期结果如下：

1） 开发者提供的准备程序，满足 5.4.2.2.1 的要求；

2） 运用准备程序能够做好产品安全运行的准备。

6.4.2.2.2 操作用户指南

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的操作用户指南，确认是否满足 5.4.2.2.2 的要求；

b) 预期结果：开发者提供的操作用户指南，满足 5.4.2.2.2 的要求。

6.4.2.3 生命周期支持

6.4.2.3.1 配置管理系统的使用

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者审查确认开发者是否使用了配置管理系统；

2） 评估者审查开发者提供的配置管理文档，确认是否满足 5.4.2.3.1 的要求。

b) 预期结果如下：

1） 能够确认开发者使用了配置管理系统；

2） 开发者提供的配置管理文档，满足 5.4.2.3.1 的要求。

6.4.2.3.2 部分产品配置管理覆盖

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的产品配置项列表，确认是否满足 5.4.2.3.2 的要求；

b) 预期结果：开发者提供的产品配置项列表，满足 5.4.2.3.2 的要求。

6.4.2.3.3 生产支持和接受程序及其自动化

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者审查确认开发者是否使用了配置管理系统；

2） 评估者审查开发者提供的配置管理文档，确认是否满足 5.4.2.3.3 的要求。

b) 预期结果如下：

1） 能够确认开发者使用了配置管理系统；

2） 开发者提供的配置管理文档，满足 5.4.2.3.3 的要求。

6.4.2.3.4 问题跟踪配置管理覆盖

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的产品配置项列表，确认是否满足 5.4.2.3.4 的要求；

b) 预期结果：开发者提供的产品配置项列表，满足 5.4.2.3.4 的要求。

6.4.2.3.5 交付程序

该项评估应遵循以下评估方法：

a) 评估方法如下：
   1） 评估者审查开发者提供的交付程序文档，确认是否满足 5.4.2.3.5 的要求；
   2） 评估者审查确认开发者是否使用了交付程序。
b) 预期结果如下：
   1） 开发者提供的交付程序文档，满足 5.4.2.3.5 的要求；
   2） 能够确认开发者使用了交付程序。

6.4.2.3.6 安全措施标识

该项评估应遵循以下评估方法：

a) 评估方法如下：
   1） 评估者审查开发者提供的开发安全文档，确认是否满足 5.4.2.3.6 的要求；
   2） 评估者审查确认开发者是否使用了文档中描述的安全措施。
b) 预期结果如下：
   1） 开发者提供的开发安全文档，满足 5.4.2.3.6 的要求；
   2） 能够确认开发者使用了文档中描述的安全措施。

6.4.2.3.7 开发者定义的生命周期模型

该项评估应遵循以下评估方法：

a) 评估方法如下：
   1） 评估者审查开发者提供的生命周期定义文档，确认是否满足 5.4.2.3.7 的要求；
   2） 评估者审查确认开发者是否使用了文档中描述的生命周期模型为产品的开发和维护提供必要的控制。
b) 预期结果如下：
   1） 开发者提供的生命周期定义文档，满足 5.4.2.3.7 的要求；
   2） 能够确认开发者使用了文档中描述的生命周期模型为产品的开发和维护提供必要的控制。

6.4.2.3.8 明确定义的开发工具

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者所提供的开发工具文档是否明确定义了用于开发产品的工具，是否无歧义地定义所有语句和实现用到的所有协定与命令，以及所有实现依赖选项的含义；
b) 预期结果：开发者所提供的开发工具文档明确定义了用于开发产品的工具，并且无歧义地定义所有语句和实现用到的所有协定与命令，以及所有实现依赖选项的含义。

6.4.2.4 测试

6.4.2.4.1 覆盖分析

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的测试覆盖分析，确认是否满足 5.4.2.4.1 的要求；
b) 预期结果：开发者提供的测试覆盖分析，满足 5.4.2.4.1 的要求。

6.4.2.4.2 测试：安全执行模块

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的测试深度分析，确认是否满足 5.4.2.4.2 的要求；
b) 预期结果：开发者提供的测试深度分析，满足 5.4.2.4.2 的要求。

6.4.2.4.3 功能测试

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的功能测试文档，确认是否满足 5.4.2.4.3 的要求；

b) 预期结果：开发者提供的功能测试文档，满足 5.4.2.4.3 的要求。

6.4.2.4.4 独立测试—抽样

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者执行测试文档中的测试样本，以验证开发者的测试结果是否正确；

2） 评估者测试产品安全功能的一个子集，以确认产品安全功能是否按照规定运行。

b) 预期结果如下：

1） 执行测试文档中的测试样本，验证了开发者的测试结果是正确的；

2） 确认产品安全功能是按照规定运行。

6.4.2.5 关注点脆弱性分析

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者执行公共领域的调查以标识产品的潜在脆弱性；

2） 评估者执行独立的产品脆弱性分析去标识产品潜在的脆弱性，在分析过程中使用开发者提供的指导性文档、功能规范、产品设计、安全架构描述和实现表示；

3） 评估者基于已标识的潜在脆弱性实施穿透性测试，确认产品是否能够抵抗具有增强型基本攻击潜力的攻击者的攻击。

b) 预期结果如下：

1） 开发者提供了适合测试的产品，并提供执行关注点脆弱性分析的相关资源；

2） 通过脆弱性分析确认产品能够抵抗具有增强型基本攻击潜力的攻击者的攻击。

附 录 A

（资料性附录）

测试样本库

A.1 病毒样本库

A.1.1 病毒样本基本库

至少包含文件型病毒、蠕虫、木马、宏病毒、脚本病毒等多种病毒类型的样本文件集合，样本文件数量不少于2000个。

A.1.2 病毒样本流行库

近三个月内流行度较高的病毒类型、病毒家族及其变种的样本文件集合，样本文件数量不少于1000个。

A.2 误报样本库

包含正常的操作系统文件、应用程序文件、数据文件等的文件集合，样本文件不少于 1000 个。

参 考 文 献

1. GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件
2. GA 243-2000 计算机病毒防治产品评级准则