瑞数信息
RIVER SECURITY

www.riversecurity.com
service@riversecurity.com | 400-611-8558

瑞数信息
RIVER SECURITY

瑞数灵控主机安全防护系统白皮书

WHITE PAPER

CONTENTS

RIVER
SECURITY

//（云）主机安全威胁及需求分析

随着网络信息技术，尤其是云计算相关技术的不断发展进步，云环境下的（云）主机安全面临着全新的威胁与挑战，安全形势日趋严峻。在云计算架构下，担负信息系统各类关键数据和核心业务系统的主机系统，一旦受到攻击，整个信息系统中最具价值的部分将面临失窃和被破坏的风险。因此，（云）主机安全已成为云计算时代公认的信息安全核心环节。

安全威胁

云服务在极大地方便用户和企业廉价使用存储资源、软件资源、计算资源的同时，也面临着巨大的安全挑战。

云服务的兴起使安全边界进一步模糊

随着云服务的日渐兴起，越来越多的业务上云，虚拟机成了安全的重灾区。虚拟化模糊了传统的安全边界，加上采用特征库比对的传统安全防护机制会大量消耗系统资源，传统的安全产品并不适合在虚拟化环境中采用。

东西向的流量攻击日渐汹涌

早期数据中心的流量，80%为南北向流量，现在已经转变成80%为东西向流量。数据中心网络流量由“南北”为主转变为“东西”为主，主要是随着云计算的到来，越来越丰富的业务对数据中心的流量模型产生了巨大的冲击。云平台内部不可视，用户无法管控虚机上的流量和应用；虚机之间缺乏威胁隔离机制，网络威胁一旦进入云平台内部，可以肆意蔓延等。

针对主机的漏洞利用攻击愈来愈多，不少漏洞遭纰漏，其中包括埋藏在系统中多年未被发现的漏洞，影响面非常广泛。

0Day漏洞带来的严重威胁

2017年4月14日，国外黑客组织Shadow Brokers泄露出了一份机密文档，其中包含了多个Windows 0Day远程漏洞利用工具，外部攻击者利用此工具可远程攻击并获取服务器控制权限，影响极大，可以覆盖全球 70% 的 Windows 服务器。根据FOFA系统统计显示，全球可能受到影响的超过750万台,中国可能有超过133万受到影响。根据白帽汇测试，从Windows2000到Windows2008都受到这工具包的影响，成功率非常之高。

WannaCry勒索病毒全球爆发

2017年5月12日，WannaCry勒索病毒事件全球爆发，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。WannaCry爆发后，至少150个国家、30万名用户中招，造成损失达80亿美元，已经影响到金融，能源，医疗等众多行业，造成严重的危机管理问题。中国部分Windows操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。

挖矿木马来势汹汹

挖矿木马缘起于数字货币，而数字货币交易价格的走高、自身隐蔽性、漏洞攻击武器种种因素，都助长了挖矿木马数量的增加。相关研究报告指出，2017年不仅是勒索软件大规模爆发，同样也是挖矿木马大肆传播之年。挖矿木马如今风头正盛，吸金力更是直追勒索病毒。

企业对于主机安全防护的意识淡薄，主机安全在管理与维护上存在不少问题。

主机组件资产数量庞大难以维护

很多互联网企业由于业务发展迅速，变更频繁，企业内部极少有人能及时了解本身的核心资产，如主机规模、域名、网段的清晰情况。尤其是资产和组织架构越来越复杂之后，管理难度就越来越高。某些大型运营商甚至连自己有多少台服务器都数不清楚。

应用系统配置风险漏洞未被重视

从近年来主机安全事件来看，应用系统的配置风险是众多用户不太重视的问题；另外随着新的应用系统类型不断增加并被应用到生产环境中，这方面的安全漏洞将会被大面积利用；这里面除了传统的数据库应用，WEB容器、开源监控系统（如Zabbix），MongoDb、Redis、Hadoop等新型应用配置风险漏洞也将成为黑客利用的目标。

采用传统安全解决方案问题重重

传统安全解决方案在传统的IT架构中发挥了较好的作用；但随着云计算的发展及虚拟化技术的应用，传统安全解决方案就存在一些较为突出的问题。传统安全解决方案无法自适应这些新的架构，无法接入虚拟化环境，需要重新进行开发。并且传统安全解决方案防御点经常是独立运作或者用户经常只部署单个防御点，无法将各个防御点很好地进行联动，导致花费了大量经费部署的安全防御措施最终还是无法防止黑客的入侵。

需求分析

通过上述针对当前网络安全现状及主机管理维护难问题的分析，我们不难发现能够满足企业实际使用需要的理想的主机安全产品需要具备有如下功能：

兼容云架构及传统架构

理想的主机安全产品需具备极强的适应性、扩展性、稳定性，支持各种虚拟化平台及虚拟机操作系统，可对物理服务器进行统一的安全管理。

主机资产采集管理

理想的主机安全产品应具备强大的主机资产采集管理能力，通过对资产信息进行分析可以为企业提供漏洞风险及入侵威胁的判断的基础信息，有助于深入发现内部暴露的问题和风险。

入侵威胁防御及处理

理想的主机安全产品应具备强大的入侵威胁防御及处理能力，面对高级攻击需能够在第一时间发现，并联动其他功能模块迅速做出响应处理。

漏洞风险检测及修复

理想的主机安全产品应具备强大的漏洞风险检测及修复能力，需能够对漏洞风险进行精准发现，并针对不同漏洞风险做出精准分析，提供精确到命令的修复建议。

基线合规性检查

理想的主机安全产品应具备强大的基线合规性检查能力，能够对主机基线进行合规性检查，对于存在安全缺陷的项目进行识别及给出相应处理意见，防止风险的产生。

// 灵控产品理念及架构

灵控主机安全防护系统（简称灵控）采用先进的自适应安全架构及端点检测及响应（EDR）解决方案，提供云+端的云安全管理平台为用户解决公有云、私有云和混合云环境中可能遇到的安全及管理问题。

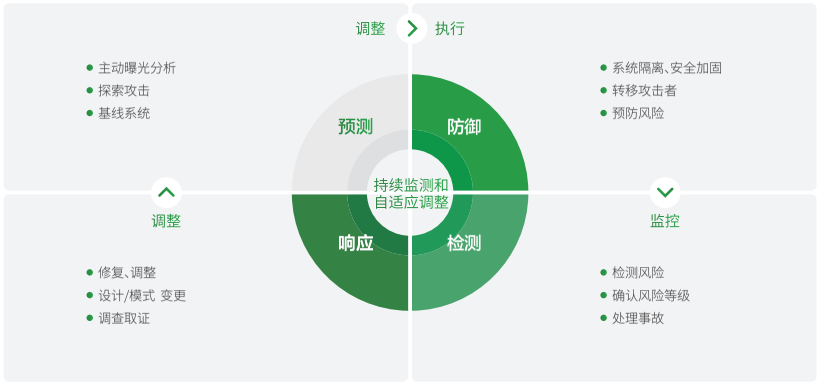
灵控产品理念

自适应安全

自适应安全是Gartner首次在2014年提出的面向未来的下一代安全架构，理念源自Gartner对美国一线安全厂商未来发展调研。大多数企业在安全保护方面会优先使用拦截和防御（例如反病毒），以及基于策略的控制（如防火墙），将危险拦截在外。但完整的防御是不可能的，系统在持续遭遇各类风险，其中高级定向攻击总能轻而易举地绕过传统防火墙和基于黑白名单的预防机制。

当前的防护功能难以应对高级定向攻击或持续攻击，持续防御能力明显不足，“应急响应”已不再是正确的思维模式，因此灵控产品的设计架构采用自适应安全架构来应对高级定向攻击。

采用自适应安全机构设计而成的灵控，集防御、检测、响应和预测于一体，以智能、集成和联动的方式应对各类攻击，而非各自为战、毫无互动。尤其对于高级威胁，自适应系统需要持续完善保护功能。



端点检测和响应(EDR)

EDR全称Endpoint Dextection and Response，即端点检测与响应，是发端于美国的下一代终端安全防护技术，该技术属于终端安全技术的重要分支之一，主要用来应对日益猖獗的APT攻击。不同于传统的杀毒软件或反恶意系统，EDR系统不会在病毒预执行阶段将其终止，而是更关注终端设备的运营状态并将其进行监控、分析、展示，以期发现各类入侵行为并对其进行相应的分析、阻断和反制等措施。

EDR系统与传统终端安全产品的工作原理存在明显改进。以杀软、防火墙等为代表的传统安全管理产品主要依据病毒的特征库、白名单以及沙箱等技术手段对恶意程序访问进行拦截，在不存在病毒、恶意程序、脚本的前提下，传统的杀软起不到任何的防护作用；此外，如今的网络攻击更有针对性，尤其是专门针对金融、工控等领域的攻击具备很强的目的性，因而传统安全防护产品的特征库中很难将此类攻击的特征信息覆盖，从而起不到防护作用。

在这种新的安全形势下，传统安全产品的防护作用日益有限，而EDR基于进程监控、多终端比对、溯源及访问分析等操作访问行为数据分析的防护理念，可以对APT等恶意攻击进行有效的提前分析、阻断，并进行溯源取证等反制措施。

EDR主要有以下三个特点：

未知威胁防护

EDR端点检测与响应产品能“点亮”主机环境，让未知威胁看得见，防得住：记录多个端点和网络事件，并将这些信息本地存储在主机、服务器或集中式数据库。政府和企业可通过机器学习、行为分析和攻击指标数据库来整合关联分析，在攻击产生危害前提前发现和预警，并对攻击做出响应。

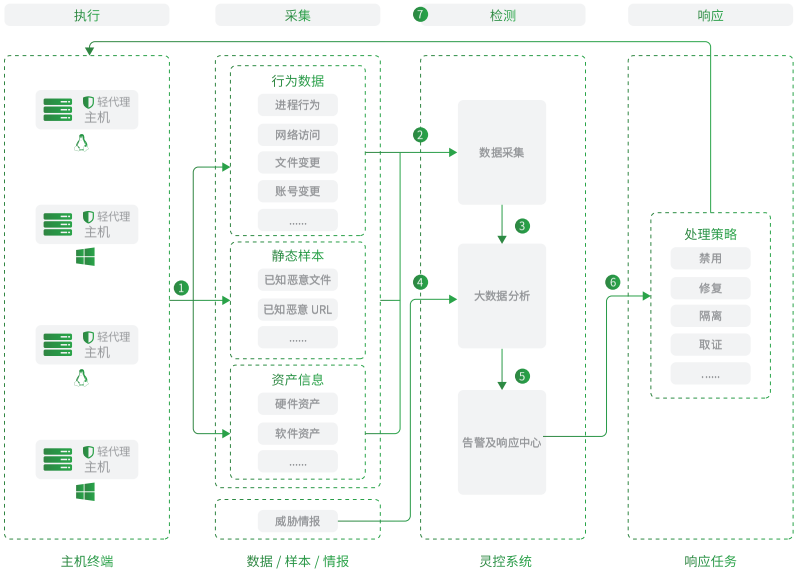
虚拟机安全

EDR端点检测与响应产品则弥补了虚拟化环境安全产品的空白：基于应用程序对操作系统调用行为进行分析，不依赖于传统静态特征防护机制，能实现未知威胁的秒级检测与响应。超轻量化安全探针，系统资源消耗量比同类产品可降低90%。从安装到运行，轻盈稳定高效。混合云跨平台统一部署管理，兼容Windows/Linux主机系统所有版本，针对虚拟化环境优化任务和资源调度，管理运维更简单省心，大幅降低“安全TCO”。

Web网站实时监测与防护

EDR端点检测与响应产品为Web网站持续监控和实时干预提供了必要手段：把检测和响应探针推到Web网站服务器，部署系统级的防护。通过“灵控人机识别”的技术对网站进行实时拍照比对，一旦发现问题便即时“熔断”，保证恶意行为不扩散。同时，通过5分钟访问流量缓存采集数据，获取黑客的攻击路径，第一时间找到漏洞以便网站快速恢复重新上线。

灵控端点检测及响应流程分为主机终端数据及信息采集、威胁情报获取、大数据分析、告警及响应四个主要步骤。



主机数据采集

通过主机端点上安装的轻代理对主机上的安全数据汇总到数据采集模块上进行统一的归类、加密，并传输给大数据分析模块。

威胁情报获取

基于瑞数公司云端的海量数据处理获取到未知威胁，并将威胁情报信息导入灵控系统大数据分析模块。

大数据分析

对主机端点采集到的安全数据结合获取到的威胁情报信息，进行威胁情报大数据分析，准确识别出威胁事件。

告警及响应

对识别出的威胁事件进行告警通知及响应处置。

灵控依靠威胁情报的指引，通过最新的安全线索快速锁定威胁主机，通过实时数据和历史主机信息对受害主机进行全面评估，揭示主机的安全缺陷，通过自动化响应机制进行处置。在威胁情报的指引下，灵控安全响应系统可以将一个复杂的高级威胁安全响应，分解成为一系列行动过程，从而解决了高级威胁难以处置的问题。

灵控“云+端”的产品架构

灵控采用云+端的云安全管理平台，为用户解决公有云、私有云和混合云环境中可能遇到的安全及管理问题；提供了包含安全体检、资产管理、漏洞风险管理、入侵威胁管理、安全监控、安全防护、合规基线、安全报表、安全告警等功能。

整体架构中包含了2个主要模块：

云：云指的是灵控系统

灵控系统是基于Hadoop构建的安全大数据平台，能够根据轻代理收集到的安全日志进行快速分析及挖掘，准确定位各种漏洞风险及入侵威胁，并第一时间进行预警。

端：端指的是轻代理

轻代理部署在服务器上（支持物理服务器、虚拟化服务器），提供多个层面的安全监控和安全保护，可快速识别及阻断黑客攻击；同时轻代理会将相应的攻击数据和日志跟云端进行联动，利用云端的大数据分析能力进一步确定是否被黑客攻击及入侵。

// 灵控产品优势

威胁情报驱动

灵控依托于瑞数动态安全系统的海量数据，以国内高水平安全研究实验室人员的技术支撑，通过机器学习与自动化数据处理技术，持续的发现未知威胁，通过统一的规范化格式将攻击中出现的多种攻击特征进行标准化并生成可机读威胁情报，用以驱动终端在第一时间内对威胁进行及时检测和响应。

分权管理规避“一权独大”

灵控采用了分权管理的机制，将原系统管理员权限分散为系统操作员、安全管理员和审计管理员，规避了原操作系统管理员“一权独大”的风险，三个权限各司其职，相互制约，保证了系统安全性，且贴合了国家相关信息安全标准规范。

多模块联动构建闭环系统

灵控拥有资产管理、安全体检、安全监控、漏洞风险、入侵威胁、合规基线、威胁情报等多个功能模块，运用采集、检测、监测、防御、捕获等各种手段对主机进行全方位的安全防护，各个模块进行联动，模块间数据联通，形成闭环系统。

采用轻量级Agent软件

灵控采用轻量级Agent，与全部功能的重量级Agent相比，轻量级Agent实现了功能的最小集合，大大减轻Agent对于主机性能的影响。并且轻量级agent简单，能够动态地升级和更新，实现的代码少，容易传输。

支持传统IT架构及云计算平台

灵控可以支持传统的IT架构，同时也支持公有云和私有云架构；目前已经与各大主流公有云平台建立合作，包括阿里云、腾讯云、青云、UCloud、AWS、华为云、天翼云、WindowsAZure等，安全套件可以应用到所有云环境中，并可以进行安全云管理。

安全高效运维

灵控提供统一Web安全管理面板，运维人员可轻松对上万台服务器进行维护管理，支持子账号创建，运维人员可将安全管理任务分配给其他人员协助管理。

全面适配Windows及Linux系统

灵控同时支持Windows2003、Windows2008、Windows2012、Windows2016等各种版的Windows系统及各种类型的Linux系统。

// 灵控产品核心功能

灵控系统的组成有资产管理、安全体检、安全监控、漏洞风险、入侵威胁、合规基线、威胁情报等多个功能模块，各个模块进行联动，模块间数据联通，形成闭环系统，为企业提供强有力的采集、检测、监测、防御、捕获能力，对主机进行全方位的安全防护。

资产管理

资产管理功能定期获取并记录主机上的端口、网站、Web容器、第三方组件、数据库、进程、账号等信息，进行统一的管理和清点。

通过资产管理功能可实时掌握IT系统内部的资产情况，支持资产变更分析对各类资产的变动情况进行记录，便于审计历史变动，自主发现异常资产行为；支持主机分组及各类资产信息标签添加；支持资产采集频率设置；支持资产信息导出；支持主机及对应资产双维度查看。

主机

灵控可自动探测业务系统中存在的主机，可采集已经安装轻代理的主机中的各类信息，可采集到的主机信息有主机内外网IP、主机名、操作系统、系统内核、业务角色、安装时间等；支持主机分组管理、资产价值设定；支持通过主机分组、体检分数、主机状态、操作系统、业务角色、资产价值、安装时间等过滤筛选。

端口

灵控可探测主机上对内端口及对外端口，可采集端口对应的服务及端口协议信息。

网站

灵控可探测主机上的网站信息，可采集网站域名、网站安装路径、网站运行状态等信息。

Web容器

灵控可探测主机上的Web容器信息，可采集Web容器的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等信息；支持Web容器有Apache、IIS、JBoss、Nginx、Tomcat、Weblogic等。

第三方组件

灵控可探测主机上的第三方组件信息，可采集第三方组件的版本、安装路径、相关网站等信息；支持的第三方组件有CKEditor、DedeCMS、Discuz、PHP、PHPMyAdmin、Struts2、WordPress、Zabbix等。

数据库

灵控可探测主机上的数据库信息，可采集数据库的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等；支持的数据有Hadoop、Memcahed、MySql、Redis等。

进程

灵控可探测主机上的进程信息，可采集进程的路径、版本、hash值等；支持进程白名单设置、业务进程设置等；可通过运行状态、进程标签、进程权限、是否系统进程、是否自启动、是否包管理安装、是否服务进程等多个维度进行进程信息的筛选。

账号

灵控可探测主机上的账号信息，可采集账号的用户名、是否Root权限、Shell、状态、上次登录时间等信息；支持业务账号设置；支持Sudo权限账号、已禁用账号、UID不唯一的账号、管理员账号、已锁定账号、非业务账号、无密码可Sudo账号、已过期账号、密码过期账号过滤筛选。

安全体检

安全体检中用户可主动发起主机深度检测，检测的项目包括：系统漏洞、弱口令、高危账号、配置缺陷、病毒木马、网页后门、反弹shell、异常账号、日志删除、异常进程、系统命令校验等。安全体检检测出的问题系统自动进行问题归类到漏洞风险及入侵威胁模块中。

支持自定义体检项体检、自定义路径体检

用户可自行选择体检项目，其中病毒木马检测支持快速扫描、全盘扫描及自定义路径扫描三种方式，网页后门检测支持自定义路径扫描。

支持即时体检及定时体检

灵控支持即时体检及定时体检两种体检模式，即时体检即检测命令下发后立即执行体检命令；定时体检用户设置扫描周期、扫描时间段后系统会按照设置规则定时执行体检命令。

支持批量体检策略下发

灵控支持批量体检策略下发，通过设置体检的类型、体检的项目、体检的主机范围进行批量体检策略下发。并且支持定时体检策略与即时体检策略两种类型。

支持体检报告生成导出

灵控支持体检报告生成及导出，体检报告展示体检分数、健康指数，体检结果图表化展示及详细体检问题说明展示，可导出Word格式的体检报告。

支持体检结果自动评分

灵控支持体检结果自动评分，通过检测的结果与预置的体检评分规则进行匹配可自动对主机健康情况进行打分，0-59分为不健康主机，60-89分为亚健康主机，90-100为健康主机。

安全监控

安全监控中用户可对主机开启各类监控包括登录监控、完整性监控、操作审计、进程监控、资源监控、性能监控。从主机安全角度，全天候监控主机的运行情况，能确保第一时间发现服务器问题，排除故障时间提速10倍，帮助企业快速发现安全风险和性能瓶颈。安全监测出的问题系统自动进行问题归类到漏洞风险及入侵威胁模块中。

登录监控

灵控对主机的登录日志进行分析，识别出主机登录流水中的异常计算机名登录、异常IP段登录、异常地点登录、异常时间登录、暴力破解登录5种异常登录行为，并且实时通知给用户。根据主机的账户登录行为分析，对可疑的登录行为提供实时告警通知。

完整性监控

灵控支持监控文件完整性，可发现删除文件、修改文件、新增文件等文件完整性异常行为；支持监控账号完整性，可发现修改账号用户名、密码等行为。

操作审计

灵控可对当前用户的输入操作进行命令审计，实时发现用户的危险操作，不依赖于传统日志的命令审计。

进程监控

支持监控服务器进程，实时发现可能存在的异常进程。

资源监控

支持监控服务器的CPU、内存、网络流量、硬盘等资源。

性能监控

支持IIS、Apache、Nginx、MySQL、SQLSever性能监控。

漏洞风险管理

漏洞风险包含两个部分，一是主机自身的安全漏洞如系统漏洞（Windows漏洞及Linux系统漏洞）、网页漏洞等；二是人为原因造成的风险因素如弱口令（操作系统弱口令、数据库弱口令等）、高危账号（高权限账号、空密码账号、用户名和密码相同的账号）、配置缺陷（操作系统配置缺陷、Web容器配置缺陷、数据库配置缺陷等）。

漏洞风险管理模块会显示当前主机上的漏洞风险情况，同时提供修复方案供用户进行参考；该模块执行时会从云端下载漏洞策略库在本地执行检测，对于存在漏洞风险的主机，会上报应用软件的名称、版本号、路径、发现时间，这个过程不会提取任何涉及用户隐私的数据。对于检测出的各类漏洞风险进行风险等级评估。

系统漏洞

Windows漏洞通过订阅微软漏洞更新，当发现主机存在漏洞时推送微软官方补丁信息，支持漏洞修复、忽略。Linux漏洞通过检测主机上的软件版本信息，与CVE官方漏洞库进行匹配，检测出存在的漏洞软件并推送漏洞信息，支持漏洞忽略。

网站漏洞

通过目录文件的检测方案，检测出Discuz远程代码执行漏洞、Discuz memcache+ssrf GETSHELL漏洞、DedeCMS注入漏洞、WordPress IP验证不当漏洞，支持漏洞忽略、修复。

弱口令

通过灵控提供的弱口令库或用户自定义的弱口令规则可发现识别操作系统弱口令、数据库弱口令、应用弱口令，支持弱口令忽略；弱口令有可能导致密码轻易被黑客或入侵者识别破译，进而成为入侵主机的快速通道，对弱口令进行检测识别并重新设置更复杂的密码，有利于保障主机安全。

高危账号

灵控通过账户防护引擎可识别发现高权限账号、空密码账号、用户名和密码相同的账号，支持高危账号忽略、禁用、信任；提权帐号的产生，很可能是系统被入侵后黑客或者入侵者对系统帐号进行了修改，及时对提权账号进行检测识别并删除提权账号，有利于保障主机安全。

配置缺陷

灵控拥有强大的操作系统、Web容器、数据库、及其他应用的配置缺陷检测能力，支持Windows2003、Windows2008、Windows2012、Windows2016等各种Windows系统配置缺陷检测，支持Memcached、CentOS、Ubuntu、Debian、OpenSUSE、RedHat等Linux操作系统配置缺陷检测；支持IIS、Apache、Nginx、Tomcat、

Weblogic、Tengine、JBOSS等各类Web容器配置缺陷检测；支持Redis、Mongodb、Memcached、Elastic-Search、PostgreSQL、Oracle等数据库配置缺陷检测；支持FTP、SNMP、Samba等应用的配置缺陷检测。各种配置缺陷的存在容易被黑客利用造成严重的损害，及时进行缺陷修复加固有助于保障主机安全。

入侵威胁管理

入侵威胁管理用以展示及处理各类入侵事件及具有高度威胁的事件，支持识别并处置的入侵威胁事件包括：病毒木马、网页后门、反弹shell、异常账号、日志删除、异常登录、异常进程、系统命令校验等。

灵控对接国内外主流查杀引擎，可检测出恶意进程及软件，并提供隔离、信任等功能。

病毒木马

病毒木马程序通常会窃取用户数据或者对外攻击，消耗大量系统资源导致业务不能正常提供服务。轻代理会采集可疑病毒木马程序的哈希指纹到云端，通过云查杀模块对哈希进行检测识别。

若确认文件是恶意的，可以对单个文件进行隔离，或者批量选择进行一键隔离，隔离成功后，原始恶意文件将被加密隔离，后期可以在隔离区进行恢复。

如果文件非恶意的，可以选择信任操作，加入信任后，灵控将不再对该文件进行检测，后期可以在信任区对信任文件进行管理。

网页后门

网站后门木马又叫webshell，一般是黑客通过漏洞入侵网站后放置的ASP、PHP、JSP等动态脚本。黑客可以通过后门木马持续控制服务器，进行文件上传下载、执行命令等各种破坏行为，对网站安全危害极大。

灵控可以实时准确的查杀各类木马恶意文件，同时提供恶意文件检测和一键隔离等功能，第一时间清除木马后门文件，确保用户服务器的安全。

反弹shell

灵控支持反弹shell检测识别及事件关闭，通过对反弹shell事件进行检测识别可入侵攻击。

异常账号

灵控支持影子账号、篡改系统账号的检测识别及事件关闭，影子账号支持禁用处理；影子账号是隐藏的账户，有管理员权限的账户，影子帐号的产生，很可能是系统被入侵后黑客或者入侵者对系统帐号进行了修改。对影子账号进行禁用处理有助于保障主机安全。

日志删除

灵控支持日志删除的检测识别及事件关闭，黑客入侵后可能对相关日志信息进行删除，检测识别日志删除事件并产生告警能够帮助安全人员及时跟进做确认。

异常登录

灵控支持异常地点登陆、异常IP段登录、异常时间登录、异常计算机名登录、暴力破解登录5种异常登录类型检测及事件关闭。异常登录意味着主机相关密码已经被窃取或破解，检测识别异常登录事件可及时发现主机风险，及时进行补救。

异常进程

灵控支持子进程权限高于父进程、隐藏进程、隐藏端口进程3种异常进程的检测识别及事件关闭。隐藏端口进程在系统中查看未能发现，但实际却在系统中被监听的端口，极大可能是系统遭遇入侵后被植入的恶意木马程序开启的服务；隐藏进程在系统中查看未能发现，但实际却在系统中运行的进程，极大可能是系统遭遇入侵后被植入的恶意木马程序。及时检测识别异常进程并关闭异常进程有助于保障主机安全。

系统命令校验

支持系统命令校验的检测识别及事件关闭；系统命令如果被恶意修改，可能会导致用户在使用系统命令时，实际使用的是被修改后的恶意程序，导致信息泄露或被入侵。及时检测识别系统命令校验事件，通过重新安装系统命令对应的包，对系统命令进行修复有助于保障主机安全。

安全防护

灵控提供强大的安全防护功能支持端口安全防护、防护控制、暴力破解防护、扫描防护、病毒防护、IP黑白名单设置、进程行为控制。通过对各类攻击事件的采集分析生成攻击趋势图、攻击分布图等图表，直观展现各类攻击事件。根据攻击事件危害程度自动匹配风险等级，并提供详实的攻击特征描述，用户可以此为参考对攻击者IP进行加黑处理，也可导出攻击事件做后续攻击分析。

端口安全

灵控支持端口安全规则设置，可选宽松模式及严格模式，宽松模式下开放所有端口，只关闭规则中的端口；严格模式下关闭所有端口，只开放规则中的端口。支持TCP、UDP、ICMP、IGMP四种协议。

访问控制

灵控支持文件保护及注册表保护，支持记录并拦截模式及记录不拦截两种模式，可选系统防护规则或自定义防护规则，系统防护规则提供高、中、低三种防护等级。

暴力破解防护

灵控提供全方位的暴力破解防护功能，支持FTP防暴力破解、远程桌面防暴力破解、MySql数据库防暴力破解、MSSQL数据库防暴力破解4种暴力破解防护功能，支持记录并拦截、记录不拦截两种模式。

扫描防护

灵控支持扫描攻击防护，能有效的防止入侵扫描，可选记录并拦截、记录不拦截两种模式。

病毒防护

灵控支持云查杀引擎、网马查杀引擎、安天本地引擎、多引擎技术识别并查杀最新病毒；可设置轻巧、中度、严格三种防护等级，轻巧防护下监控程序执行和网页文件写入，确保病毒无法运行，对系统性能无影响；中度防护下监控程序执行、写入，网页文件写入，确保病毒无法入侵，对系统性能影响小；严格防护下监控对程序和网页文件任何形式的访问，对系统性能会有一定影响。支持自动隔离（在隔离区备份原文件）及不处理（只写日志）两种处理方式。

IP黑白名单

灵控支持白名单及黑名单设置，支持黑白名单批量导出及导入；黑名单下可设置记录并拦截、记录不拦截两种模式。

进程行为控制

灵控支持进程行为控制，能够有效的防止非法进程操作。

合规基线

在等级保护检查、测评、整改工作过程中，对定级业务系统进行对应级别的安全风险检查是技术方面的必要工作，通过使用灵控的合规基线功能进行基线检查即可轻松完成。

灵控对国家等级保护规范进行了详细整理，把技术标准落实到每一种应用的配置检查工作上。灵控结合等级保护工作过程，对业务系统资产进行等保定级跟踪，根据资产定级自动进行对应级别的安全配置检查，对合规情况出具等保符合性报告，保证系统建设符合等保要求，促使等保监督检查工作高效执行。

提供官方等保基线模板，满足等保二级及等保三级要求。
支持用户自定义基线模板。
支持合规基线检查策略批量下发。

威胁情报

灵控威胁情报来自瑞数云端的分析成果，针对高级持续性威胁、新型木马、特种免杀木马进行规则化描述。威胁情报通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌，包括程序形态，不同编码风格和不同攻击原理的同源木马程序、恶意服务器（C&C）等，通过全貌特征‘跟踪’攻击者，持续的发现未知威胁，最终确保发现的未知威胁的准确性，并生成了可供大数据分析平台使用的威胁情报。

安全报表

整体网络态势感知，根据主机有无被入侵、是否有监控异常、体检不健康主机数评判当前整体网络态势；
自定义时间区间分析生成全站攻击趋势、攻击类型分布、资产分布、漏洞风险分布、漏洞发现趋势、入侵威胁分布、入侵威胁发现趋势、新增监控异常分布、监控异常变化趋势等图表。
支持全站安全信息报表生成导出。

// 灵控相关参数

资产发现与采集支持情况

类别	版本	支持情况
主机	Windows 2003	Web Edition、Standard Edition 、Enterprise Edition、Datacenter Edition
	Windows 2008	ALL
	Windows 2012	Foundation、Essentials、Standard、Datacenter
	Windows 2016	Essentials、Standard、Datacenter
	Ubuntu	11.04、12.04、14.04
	Centos	5.4--7.3
	RedHat	4-6
	Fedora	支持
	Suse	支持
	Debian	支持
WEB 容器	Apache	2.0（Windows）、2.2、2.4
	IIS	6.0、7.0、8.0
	Nginx	1.0、1.2、1.4、1.6、1.7、1.8、1.9、1.10、1.12
	Tomcat	支持
	Weblogic	支持
	JBoss	支持
数据库	Memcached	支持
	Mysql	支持
	Hadoop	支持
	Redis	支持
	ElasticSearch	支持
	Hbase	支持
	PostgreSql	支持
	MongoDB	支持
	Oracle	支持
	SqlServer	支持
第三方组件	CKEditor	支持
	DedeMS	支持
	Discuz	支持
	PHP	支持
	PHPMyAdmin	支持
	Struts2	支持
	WordPress	支持
	Zabbix	支持
	RabbitMQ	支持
	zookeeper	支持
	Dubbo	支持
	Kafka	支持
	Jenkins	支持
	fastJSON	支持
	git	支持
	svn	支持

漏洞风险支持情况

类型	说明
系统漏洞	漏洞支持 Windows、Linux； Linux 包括 rootkit 漏洞、Linux 核心库漏洞、Linux CVE 漏洞等； 支持自动扫描云主机操作系统的系统漏洞，并提供补丁下载； 支持安全建议、漏洞介绍、影响版本、CVE、CVSS、漏洞描述及修复；
弱口令	支持 ssh、RDP、MySQL、FTP、Redis、MongoDB、Memcached、ElasticSearch、PostgreSQL、Samba、VSFTP、ProFTP 的弱口令检测
高危账号	可对系统中的影子账号、空密码账号、可疑高权限帐号、可 sudo 账号、是否限制 su 成 root 帐号检测和告警
WEB 容器	支持 nginx、apache、weblogic、tomcat、Jboss 配置风险监测
组件漏洞	MySQL、Redis、Dubbo、ElasticSearch、Kafka、Memcached、Nginx、PHP、Hadoop、Jboss、Struts2、PostgresSQL、Jenkins、Weblogic、zabbix、fastJSON、git、svn、IIS、jetty
CMS 漏洞	支持 Wordpress、Discuz、phpmyadmin、DedeCMS 漏洞检测及修复
暴力破解	已支持 SSH、Mysql、RDP、FTP 防暴力破解 其他暂无计划:SQL Server、Redis、Mongodb、Memcached、ElasticSearch、Samba、snmp

基线检查支持情况

项目	类别	支持情况
Windows	Windows 2003	支持
	Windows 2008	支持
	Windows 2012	支持
	Windows 2016	支持
Linux	Ubuntu	支持
	Centos	支持
	RedHat	支持
	Fedora	支持
	Suse	支持
	Debian	支持
WEB 容器（linux）	Nginx	支持
	Apache	支持
	Weblogic	支持
	Tomcat	支持
	Jboss	支持
WEB 容器（Windows）	IIS	支持
	Apache	支持
	Tomcat	支持
数据库基线	Mysql	支持
	MongoDB	支持
	Redis	支持
	ElasticSearch	支持
	Hbase	支持
	postgres	支持
	mongodb	支持
第三方组件	nginx	支持
	apache	支持
	weblogic	支持
	tomcat	支持
	Jboss	支持

瑞数灵控主机安全防护系统
白皮书

瑞数信息
RIVER SECURITY

关于瑞数信息

瑞数信息（River Security）成立于 2012 年，是国内创新推出动态安全，全程动态保护企业业务安全的供应商。总部位于上海，在北京和深圳分别设有分支机构，并在成都设立研发中心。

瑞数全球领先的“动态安全”防护技术，完全颠覆了传统安全依赖攻击特征与策略规则的被动式防御技术，可有效协助企业对抗现有安全技术无法有效应对的新兴威胁，打击伪装正常交易的业务作弊、利用合法帐号窃取敏感数据及假冒合法终端应用的各类网络欺诈与攻击行为，保护在线交易与企业网站的安全。

网络空间中的欺诈行为，除了业务层的欺诈外，也有可能通过窃取网站数据、误导用户使用非法第三方应用或在网络上进行中间人攻击等手段进行欺诈。唯有对交易过程中的业务层、应用层、网络层及访问终端进行全面覆盖，才能有效解决网络空间中面临的各类新兴欺诈威胁。

瑞数动态安全采用创新的“ 动态安全 ”理念，防护能力不只是增加目标系统的不可预测性，更能根据威胁态势对交易的全过程进行动态感知、分析与预测，即时追溯与阻断恶意攻击来源，能更高效地防护各类数字化时代的新兴威胁。