★完全公开

奇安信网神云锁服务器安全管理系统 V8.0
产品白皮书

V8.0.5

首次创建时间：2021 年 7 月 8 日
最新修改时间：2022 年 3 月 1 日

地址：北京市西城区西直门外南路26号院1号

邮编：100044

版权声明

免责声明

本免责声明（**“本声明”**）适用于奇安信集团（包括但不限于**奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司**，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称**“本产品”**）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论**

是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利：**在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**

8. 本声明受中华人民共和国法律的约束并依据其解释。

9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0.0	C	新建	赵舶程	周灿	2021-08-30
V1.2.0	A	新增 8.0.5 部分内容	赵舶程	杜磊	2022-03-01

状态：C-创建，A-增加，M-修改，D-删除

目 录

1 服务器安全背景

在目前的网络安全大环境下，传统防护手段和防病毒安全系统已经无法承载日新月异的威胁攻击。为了确保企业的业务连续性，避免病毒对企业的数据、应用、网络等资产带来威胁，必须对企业的主机安全系统进行结构化的完善，企事业单位主要面临以下挑战：

一是服务器资产家底不明，由于企业在信息化方面的投入不断增加，IT 资产也随之增涨。早几年里，企业的安全运营人员面对机房里的资产管理还能从容应对。如今，如果对资产管理的重视程度和运营方式还停留在以前的水平，迟早会成为黑客的下一个目标；

二是服务器资产暴露公网不知，如果要入侵一台服务器，从开放的端口服务下手；那么，如果要入侵一家企业，从互联网暴露面资产进行探测，主要围绕域名、IP 进行信息收集。不少企业因各种历史遗留问题，如业务端口开通没有进行登记管理、项目交接、人员调动等客观因素，导致企业外网资产一直存在混乱状态，隐形资产成为了攻击者的切入点；

三是服务器漏洞层出不穷，据 CNNVD 统计，仅 2020 年被曝出漏洞就达 29320 个，这只是冰山一角，多数客户面对 0day 漏洞、未知漏洞时，缺乏有效防护手段；

四是服务器遭受攻击后无法止损和溯源，一旦企业中的某台服务器被攻破或遭受到勒索病毒攻击，攻击者会在内网扫描入侵更多机器进行横向爆破，但由于失陷主机受控或发起恶意行为往往难寻规律、隐蔽性极强，只能被动的等待问题发生后进行补救，同时黑客攻击技术越发精深、手段越发高超隐蔽，无法在第一时间精确的定位攻击者；

五是补丁周期滞后且无法覆盖已知所有漏洞，截止到 2020 年 12 月尚有 2018 的 5056 个漏洞未补，犹如定时炸弹，随时可能引爆，同时政企客户场景非常复杂，打补丁后经常出现程序不兼容甚至系统崩溃等现象。

结合以上的服务器安全防护痛点，我们可以得出，安全总是相对的，再安全的服务器也有可能遭受到攻击，系统遭受攻击并不可怕，可怕的是面对攻击束手无策，所以对于 IT 管理人员来说，公司服务器的运行，包括从运维人员运维到

操作系统自身的整个生命周期，均存在安全隐患，所以应构建整体的主机安全防御体系，需从网络安全、数据安全、业务安全、应用安全、中间件安全、操作系统安全多个层次出发，才能达到整体安全防御的效果。

2 产品设计理念与架构

2.1 产品简介

奇安信网神云锁服务器安全管理系统是中国用户总量领先的主机安全产品，在国际上率先达到 Gartner 定义的 cwpp（云工作负载保护平台）标准、EDR(终端检测与响应)+EPP(Endpoint Protection Platform)标准，兼容多种虚拟化架构和操作系统，可以高效支撑现代混合数据中心架构下的主机安全需求。

奇安信网神云锁服务器安全管理系统是一款服务器主机综合防护软件，采用轻量化 Agent 技术，通过对主机的暴露面梳理和持续威胁监测分析，可在第一时间精准发现服务器安全威胁及入侵事件，可提供服务器等保合规、勒索挖矿、弱口令及风险账号治理、恶意扫描、爆破登陆、提权、无文件攻击、Webshell/反弹 shell、文件篡改、文件泄露、病毒横向扩散、补丁空窗期治理、软件漏洞等场景的统一解决与处置方案，使服务器在满足等保合规的基础上，有效防止各类恶意入侵及破坏性攻击，同时具备自主杀毒引擎+集成主流杀毒引擎，提供全面的服务器勒索、挖矿治理能力。

2.2 产品设计理念

奇安信网神云锁服务器安全管理系统（以下简称“云锁”）以攻击者的角度，并结合 ATT&CK 进行综合分析，搭建攻击面分析、纵深防御、分析监控、应急响应的综合防御体系。如下图所示：

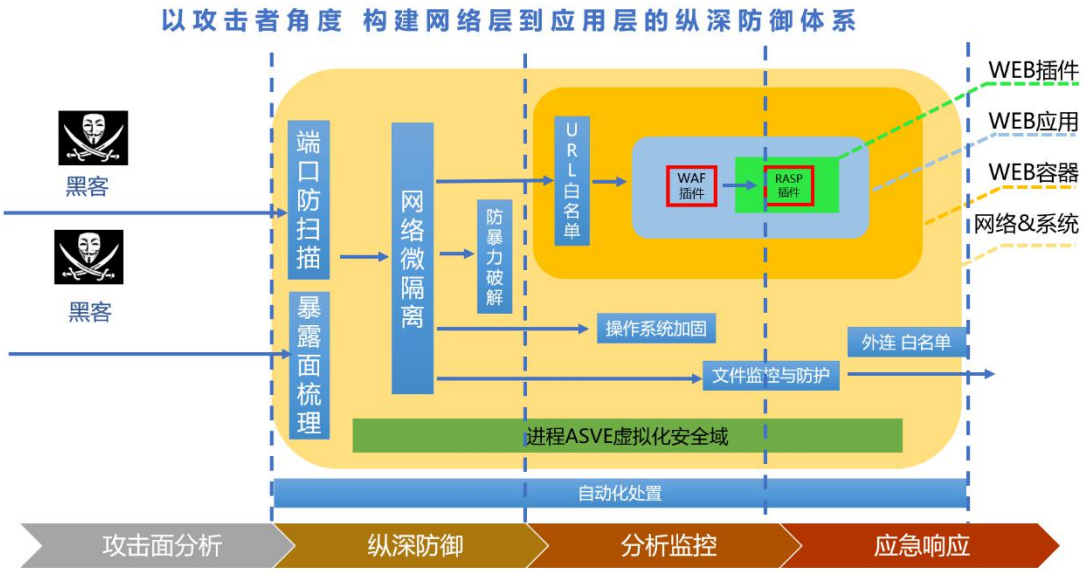


图 1 设计理念

同时，云锁吸收了传统主机入侵检测系统的优秀思想，将安全、管理、运维思想进行融合，以“三加强，三防护”的安全理念，结合服务器全层次安全防护、安全运维管理手段，融合安全技术，达到服务器“外防输入、内防扩散”的效果，构筑服务器安全生态。如下图所示：

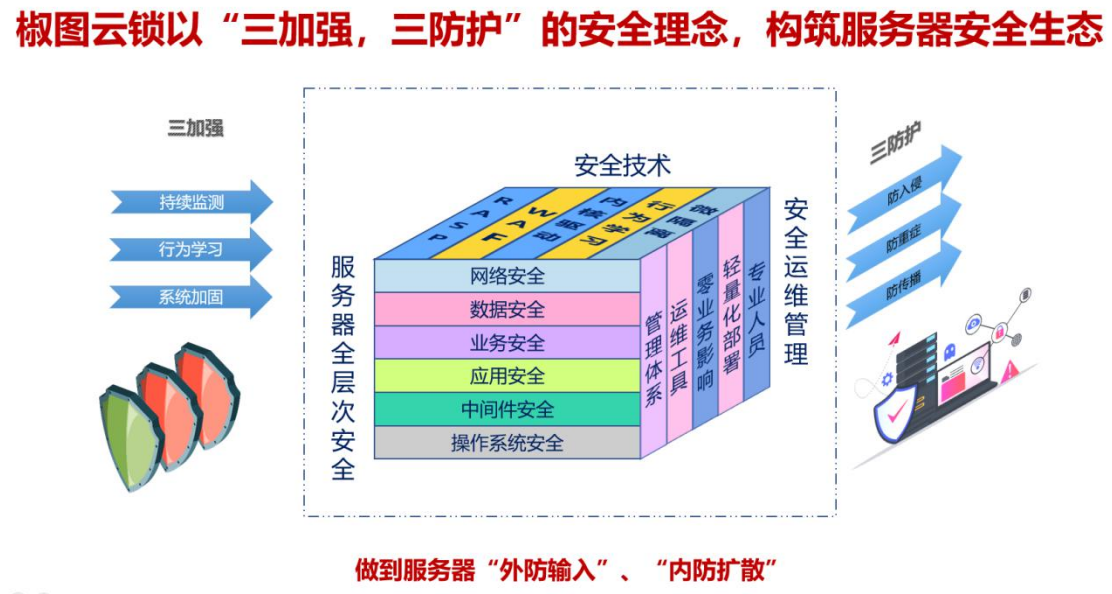


图 2 技术-安全-管理-运维相融合

2.3 产品应用场景

奇安信网神云锁服务器安全管理系统是一款用于对政府、金融、能源、电力、交通、运营商等大型企事业单位服务器的立体化安全检测与防护系统，提供资产

梳理、暴露面梳理、风险发现、威胁监测、病毒查杀、等保合规基线、系统加固、溯源分析等全面的安全能力，在服务器端形成、事中控制、事后溯源的一体化防护体系。全面覆盖服务器资产梳理、暴露面梳理、漏洞检测、病毒查杀、勒索病毒防护、等保合规、服务器微隔离、日常运维等 12 种场景。如下图所示：

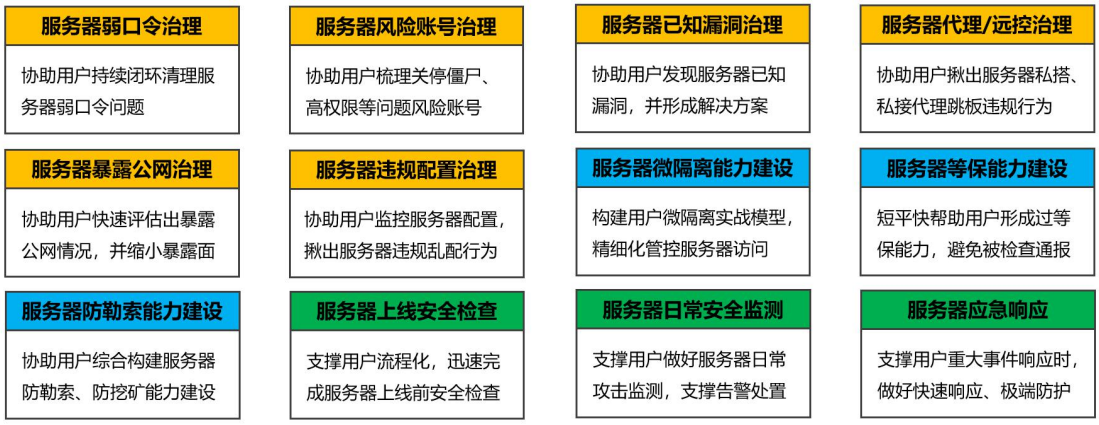


图 3 产品应用场景

2.4 产品形态及架构

奇安信网神云锁服务器安全管理系统为纯软件形态，云锁采用轻量化 Agent、管理控制中心结合的方式，为用户解决物理服务器、虚拟服务器环境中可能遇到的服务器管理问题、安全问题、合规问题。系统架构如下图所示：

图 4 产品形态和架构

整体架构分为三部分：

1、Agent 客户端：

云锁基于无感化 Agent 技术，部署在被防护的服务器上（支持物理服务器、

虚拟化服务器），具有反逆向、反调试、自保护功能，支持私有化防护场景，提供多个层面的安全监控和安全保护，可通过接收管理控制中心下发的处置策略快速识别及阻断服务器攻击。默认情况下运行时 CPU 占用不超过 10%，内存占用不超过 200MB。agent 和管理平台通信采用安全的加密机制。Agent 支持停用与卸载行为的告警。

2、云锁管理控制中心：

云锁管理控制中心系统是基于 Hadoop 构建的服务器安全大数据分析平台，可根据 Agent 客户端收集到的安全行为和日志进行快速分析及挖掘，准确定位服务器异常行为和安全风险以及入侵威胁，并第一时间进行预警，统一管理 agent 的卸载、禁用、启用、重启等操作。同时可下发对服务器端口、IP、文件、应用的处置策略，可在第一时间对受攻击的服务器进行阻断及隔离，防止横向感染。管理平台账号包含管理员、审计员、普通用户等三个角色。

云锁管理控制中心系统支持集群部署，支持 6000 点以上 agent 管理。

奇安信网神云锁服务器安全管理系统_单节点安装部署环境要求		
分类	配置项	配置要求
椒图云锁管理控制中心服务器	操作系统	CentOS7.0 以上 X64
	CPU	x86 架构 Cpu 16 核及以上
	内存	32G 以上内存
	硬盘	500 以上空余硬盘空间
受保护的客户端	操作系统	Windows Server 2003 及以上 Linux/Redhat/Centos/中标麒麟/银河麒麟/统信
	CPU	x86 架构 Cpu 即可
	内存	4G 以上内存
	硬盘	200G 以上空余硬盘空间

3、接口/API：

（1）云锁提供多种方式的 API 接口，支持以 syslog 的方式将系统登录日志、网络行为日志、系统加固日志、文件操作日志、进程操作日志、网络攻击日志、外连设备监控日志、威胁感知事件等日志，推送至天眼、NGSOC 平台进行数据协同分析；

（2）可支持天眼下发 IP 黑名单至管理中心的[网络防护--ip 黑白名单]中，并自动阻止黑名单的一切访问与操作；

（3）可支持天眼从内外网流量中监测到弱口令信息（例如内网访问浏览中存在 password=123456 口令）发到云锁控制中心，并根据弱口令信息对所有主机进行弱口令联动扫描；

（4）支持 NOSOC 从椒图云锁中自动获取 15 类资产信息，并在 NGSOC 资产中心或大屏中展示。

2.5 产品核心技术

2.5.1 资产发现与测绘技术

资产发现与测绘技术，通过主动探测和被动识别的两种方式，从多维度对资产进行探测，管理中心通过自动或人工的方式下发资产收集任务给 agent 端，该任务由若干负责资产收集的 lua 脚本组成。agent 通过执行任务中的 lua 脚本，完成主机上各类资产的收集工作。同时还可通过同网段内的 Agent 自动扫描技术，对未安装 Agent 的资产进行发现，从而发现未安装 Agent 的主机。

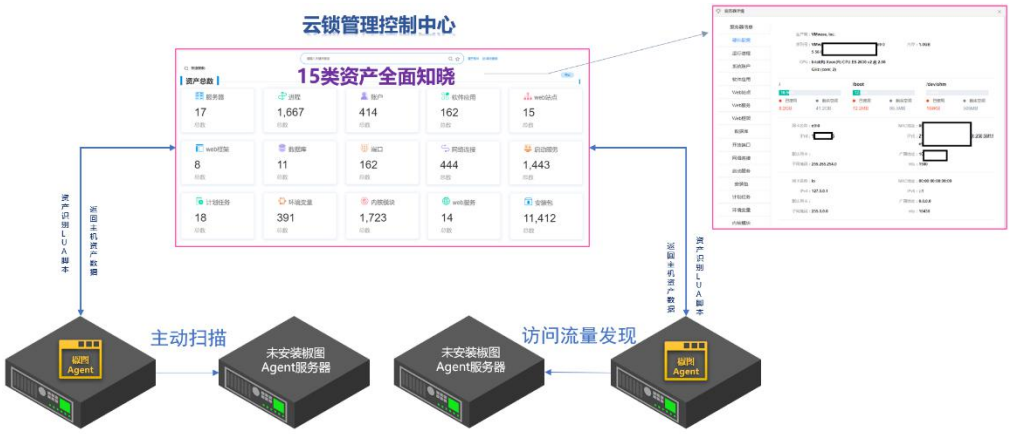


图 5 资产发现与探测技术

通过对资产的发现与测绘分析技术，实现了对服务器资产、进程、账户资产、软件应用、web 站点、web 框架、web 服务、数据库、端口、网络连接、启动服务、计划任务、环境变量、内核模块、安装包等多个纬度对服务器资产进行全面清点，并对没有安装客户端的服务器进行识别，解决了服务器资产无法精确盘点、无法知晓的问题。

2.5.2 服务器异常行为分析技术

采用服务行为识别和分析技术，通过关联主要服务名称（路径）和端口号对服务器的网络外连，命令执行，文件创建等行为进行监控和学习，并形成行为基线白名单策略，当服务器存在漏洞并被黑客利用后，产生非白名单范围内的网络外连，命令执行，文件创建等行为（偏离行为基线），系统可进行阻断或告警。如下图所示：

图 6 服务器异常行为分析技术

通过对服务器服务行为识别分析和判断，实现了白名单行为自主学习，对异常服务行为进行监控告警，解决了攻击者通过混淆服务的行为对服务器发起的攻击。

2.5.3 应用 WAF 探针技术

In-app WAF（嵌入式 WAF）是通过插件的方式，工作于 IIS、Apache、Nginx 等 web 中间件内部，持续监控 HTTP 层的请求流量，通过流量特征判断以及 WAF 规则引擎匹配 HTTP 请求里隐藏的攻击载荷，从而对访问流量进行防护。如下图所示：

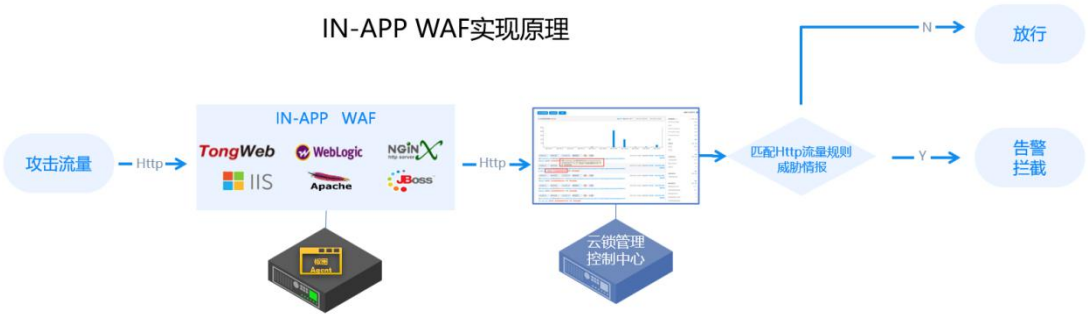


图 7 应用 WAF 探针技术

通过 In-app WAF 内置于 web 中间件，赋予 web 应用内在安全检测防护能力，将访问流量进行解析并与内置的攻击规则进行匹配，实现对 SQL 注入、XSS 跨站、溢出攻击、应用漏洞攻击进行 WEB 综合防护，不但解决了传统网络 WAF 对 web 应用程序漏洞被绕过无感知的问题；还解决了恶意流量被旁路绕过、加密流量无法检测的问题。

2.5.4 虚拟补丁技术

虚拟补丁技术在不修改应用程序源代码、修改二进制代码或重新启动应用程序的情况下，能够即时建立的一个安全策略实施层，用来防止对已知漏洞的攻击。防护原理如下图所示：

图 8 虚拟补丁技术

使用虚拟补丁技术，组织可以在大幅减少补丁所需的成本、时间和工作之间取得很好的平衡，同时保持服务的可用性和正常的补丁周期。

2.5.5 应用动态防护 RASP 技术

RASP（应用运行时自防护）提供对应用上下文信息分析判断解析的能力。RASP 工作于 ASP、PHP、Java 等脚本语言解释器内部，通过 HOOK 钩子函数的方式，细粒度的监控应用脚本的行为以及函数上下文调用信息。通过对 web 应用的文件读写、命令执行、数据库操作、网络连接等行为进行监控，当发生异常行为时，通

过对 web 请求的上下文进行分析，实现对威胁行为的检测及处置。如下图所示：

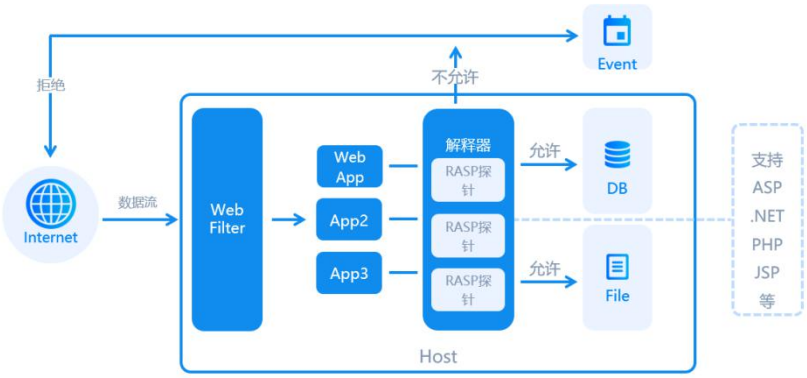


图 9 应用动态防护 RASP 技术

通过 RASP 应用运行时自防护模块，基于分析流量上下文、执行行为特征检测，使应用程序能够自我监控和识别有害的输入，解决了传统 WAF 的防护策略依赖特征和安全规则，而对于 0day 漏洞和新型恶意代码没有防护能力的问题。

2.5.6 系统内核驱动加固技术

内核加固技术，通过 hook 技术对系统 I/O 请求进行过滤检测，匹配访问控制规则，实现对特定进程文件、注册表的操作的监控与防护，可以对服务器系统安全涉及的控制点实现访问控制限制，防止黑客利用应用漏洞进行提权、创建可执行文件等操作。有效防止原本可信的【白应用】被【黑利用】。如下图所示：

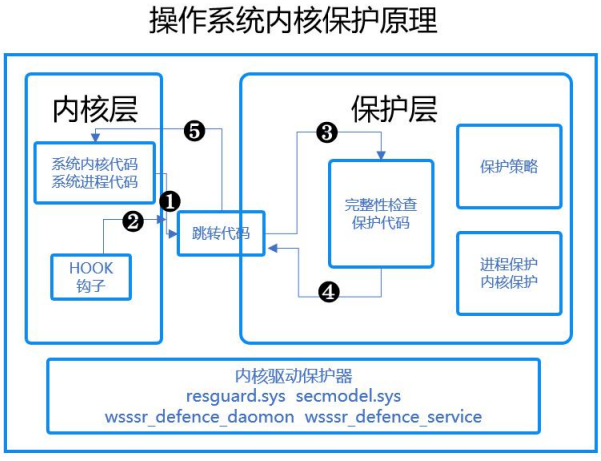


图 10 系统内核驱动加固技术

通过构建操作系统的保护层，可确保系统中的信息执行和系统自身的安全性，解决操作系统层面和内核层面面临的恶意代码执行、越权访问、数据泄露、破坏数据等行为，保障操作系统的保密性、完整性、可用性、可靠性。

3 产品优势

3.1 主机资产动态掌握

奇安信网神云锁服务器安全管理系统能够帮助企业自动清点主机资产状况，快速了解业务系统情况。实时动态掌握服务器资产中存在的各类风险以及暴露的问题，方便用户快速检索特定的资产详情或相关风险。通过主机发现，系统可将自动扫描已经安装的探针主机，所在网络空间未纳入安全管理的主机，自动排除普通网络设备，保证探测与被探测主机正常运转。

3.2 领先的未知威胁响应能力

1、未知威胁检测：通过对应用系统的日志、上下文、行为进行持续监控，识别并防御已知、未知威胁。能有效防御 SQL 注入、命令执行、文件上传、任意文件读写、反序列化、Struts2 等基于传统签名方式无法有效防护的应用漏洞。

2、立体化防护：通过持续监控和行为识别为核心，对管理中心平台回传的行为数据进行智能分析，完成对应用攻击的预测，防御，监控和回溯，实现立体化纵深防御体系。

3.3 部署方式灵活可用性高

奇安信网神云锁服务器安全管理系统结合客户网络现状，支持外网、内网及混合网络的产品交付。采用业务优先原则，产品以轻量级代理的方式部署到服务器中，占用系统资源少，支持 Syslog 协议或标准化接口用于安全管理与态势感知平台的联动。

3.4 兼容多种操作系统及业务环境

支持 windows server2003 及以上 windows 服务器操作系统；支持 centos、Ubuntu、redhat、中标麒麟、红旗 linux 等超过 280 个 linux 内核版本。

3.5 自适应识别多种业务应用

支持 IIS、apache、nginx、tomcat、weblogic、websphere 等主流 web 中间件以及 MySQL、SQL server 等数据库应用，并自动化匹配安全规则。

4 产品功能

4.1 资产管理

4.1.1 资产信息

资产信息功能可自动收集服务器上的资产信息，包括服务器基础信息，操作系统，进程，账户，web 站点，web 应用，服务，服务版本，Web 框架，端口，网络连接，软件应用，数据库，启动项，安装包、计划任务，环境变量，内核模块、注册表、证书资产、类库资产等资产信息，可帮助用户快速了服务器各类资产详细信息，提供关键词资产信息搜索和导出。

4.1.2 资产收集

资产收集可支持以定时任务的形式，收集服务器资产的进程，账户，web 站点，web 服务，Web 框架，端口，网络连接，软件应用，数据库，启动服务，安装包、计划任务，环境变量，内核模块等信息，可对资产类型、目标服务器、收集频率、采集时间进行设置。

自动清点服务器存在的数据库信息，包括：主机 IP、数据库版本、监听端口、运行用户、配置文件路径、绑定 IP 地址、启动参数等。

数据库类别包括：MySQL、Redis、MongoDB、Oracle、PostgreSQL、Hbase、SQL Server、TiDB、DB2。

自动清点系统中配置的包括 Linux 系统的 crontab、at、batch 和 Windows 系统的 schtasks 等计划任务，并按照任务类型进行分类。

4.1.3 主机发现

通过主机发现，系统可将自动扫描已经安装的探针主机，所在网络空间未纳入安全管理的主机，自动排除普通网络设备，保证探测与被探测主机正常运转。

4.1.4 分组管理

分组管理可根据现有的服务器业务实际情况，进行服务器资产分组标签管理，通过对服务器分组后，可在服务器列表中看到服务器的所属分组，并可根据分组进行查询。

4.1.5 后台 URL 梳理

可对服务器的业务后台 URL 进行梳理，可自定义 Url 关键字和 POST 关键字，当匹配到关键字时，将自动加入后台 URL 列表，支持用户手动添加和自动学习生成。

4.1.6 资产变更

对安装 Agent 服务器的账号、端口、计划任务的变更进行监控，包括：变更时间、所在服务器名称、变更类型、变更内容、变更详情等信息，并提供搜索及导出功能。

4.2 行为管理

4.2.1 服务行为

服务器行为基于机器学习的行为模式，帮助用户管理重要业务服务列表，梳理对外服务进程及其子进程进行的命令执行，文件创建，网络外连操作行为，同时可帮助用户快速梳理整个业务信息系统的暴露面，对端口进行访问控制，对异常 IP 的告警或阻断。同时自动监控全网服务器进程成功外连行为并记录日志。

4.2.2 应用白名单

应用白名单可对一台或一组服务器创建智能学习的应用白名单策略，并对白名单以外的应用进行告警和拦截，可防止攻击者通过混淆服务的行为对服务器发起的攻击。

4.3 微隔离

4.3.1 防火墙

对服务器的入流量和出流量的访问控制进行告警，包括：服务器名称、最近访问时间、在线状态、系统类型、服务器 IP、所属分组、原地址、目的地址/域名、网络协议、规则名称/域名、访问告警记录等信息，并可对服务器配置相关的防火墙访问规则，包括对 IP 地址的出入方向、端口、IP 进行配置，和域名的禁止和运行配置，并可对服务器的防火墙功能进行开启、关闭、策略下发等功能。

4.3.2 端口白名单

可对外网、内网暴露的端口进行梳理，并支持暴露控制策略配置，包括：禁止/允许外网暴露、禁止/允许内网暴露等策略，还可设置例外端口，以便业务的正常访问。

4.3.3 外连白名单

外连白名单可自动分析服务器上连接外网 IP 和域名，并根据收集的信息创建白名单，当连接的外网 IP 或域名不在白名单内，则产生事件告警。

4.4 风险发现

通过风险扫描功能对服务器的 webshell、后门、漏洞，弱口令等风险进行检测，发现服务器上的风险异常。并通过风险管理功能，进行统一查询，筛选及处置。能够定时为用户提供风险报告输出。

4.4.1 账户及口令风险

账户风险可对服务器中的风险账户进行检测，发现可能存在风险的账号，包括：高权限账户、过期账户、默认账户被启用、可远程账户、克隆账户、隐藏账号等

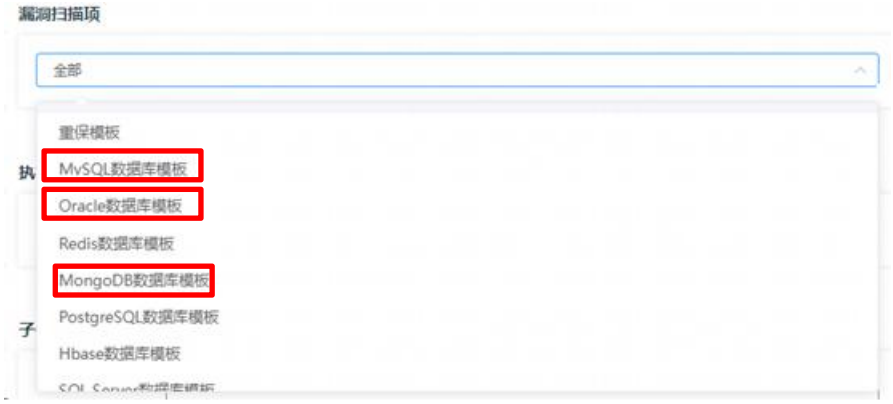
口令风险可对服务器以及服务器上应用的弱口令进行扫描，内置主流的弱口令字典，并支持自定义用户名字典和口令字典。支持口令的修复验证，同时可对网内中复用的口令进行排查和检测，规避口令复用风险。包括检测操作系统服务、数据库、中间件的弱口令。

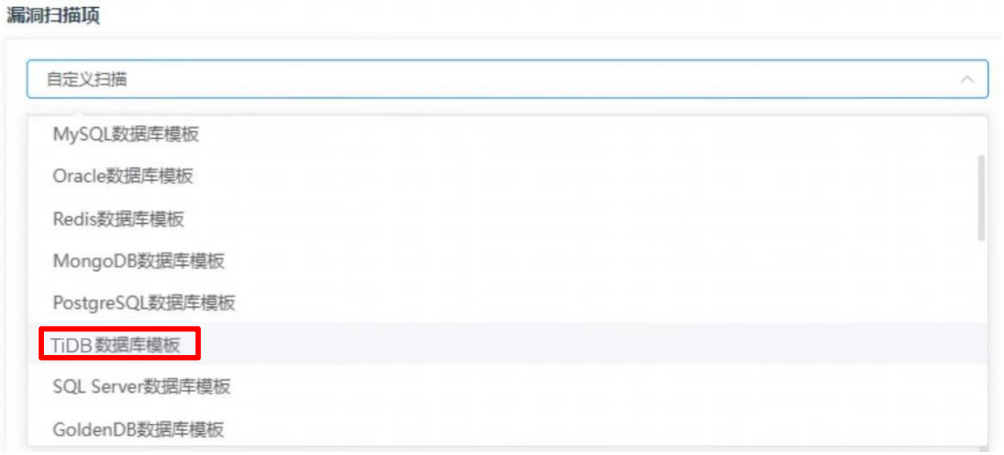
4.4.2 软件漏洞

1、 软件漏洞检测可对软件漏洞进行扫描，内置 500 余种主流软件漏洞检测，并。支持版本号识别和指纹识别和自定义扫描和全盘扫描等多种方式兼容 CVE、CNNVD 等国内国际规范的漏洞信息，同时提供了重保软件漏洞扫描模板，可为重保模式下提供软件漏洞扫描。漏洞类型包括但不限于操作系统漏洞（Windows、Linux 等）、数据库漏洞（MySQL、Oracle、TiDB、MongoDB 等）、Web 容器漏洞（Tomcat、Apache、Ngnix 等）及其他组件漏洞。漏洞信息包括：CVE 编号、资产信息、漏洞级别、漏洞名称、漏洞类型、利用特征等。提供补丁的详细信息，包括补丁的修复建议、补丁安装的依赖关系、修复命令、修复影响，补丁当前版本和修复后版本，提供内核风险、是否存在 EXP、远程利用、本地提权，以及相关的 CVE 编号等补丁风险特征。

规则ID	规则名	操作系统	漏洞编号	类型	影响
63823950	Struts2远程代码执行漏洞(S2-005)	Windows，Linux	CVE-2010-1870	其它	Web应用程序攻击
61041978	Windows SMB server_message_block远...	Windows	CVE-2017-0144	操作系统	管理员权限获取尝试
61041984	Microsoft Windows SMBv1 安全漏洞	Windows		:系统	管理员权限获取尝试
61042294	Microsoft Windows SMBv1 安全漏洞	Windows		:系统	管理员权限获取尝试
61042944	Microsoft Windows SMB 远程代码执行漏洞	Windows	CVE-2017-0146	操作系统	管理员权限获取尝试
63019108	Microsoft Windows SMB 输入验证漏洞	Windows	CVE-2017-0148	操作系统	用户权限获取尝试
61002015	EMC NetWorker 'librpc.dll'动态库信息泄漏...	Windows	CVE-2011-0321	其它	RPC查询解码
61007070	Microsoft MVC 跨站脚本漏洞	Windows，Linux	CVE-2014-4075	中间件	Web应用程序攻击
61010192	RealPlayer 'IERPPLUG.DLL' ActiveX控件...	Windows	CVE-2006-6847	应用	用户权限获取尝试
61010193	RealPlayer 'IERPPLUG.DLL' ActiveX控件...	Windows	CVE-2007-5601	应用	用户权限获取尝试
61010194	RealPlayer 'IERPPLUG.DLL' ActiveX控件...	Windows	CVE-2008-3066	应用	用户权限获取尝试
61011259	BarCodeWiz BarcodeWiz.dll ActiveX Cont...	Windows	CVE-2010-2932	其它	用户权限获取尝试

漏洞类型：windows、liunx





规则ID	规则名	操作系统	漏洞编号	类型	影响
61017387	Apache Tomcat UTF-8 目录遍历漏洞	Windows，Linux	CVE-2008-2938	web服务器	可疑文件名
61017391	Apache HTTP Server Tomcat远程目录...	Linux	CVE-2007-0450	web服务器	Web应用程序攻击
61018096	Apache Tomcat表单认证用户名枚举漏洞	Windows，Linux	CVE-2009-0580	web服务器	信息泄露尝试
61028532	PyLoris tomcat http DoS tool	Windows，Linux	CVE-2012-5568	web服务器	拒绝服务攻击尝试
				web服务器	用户权限获取尝试
				web服务器	用户权限获取尝试
				web服务器	Web应用程序攻击
63019149	tomcat远程代码执行漏洞	Windows，Linux	CVE-2017-12615	web服务器	管理员权限获取尝试
63019186	apache tomcat远程代码执行	Windows	CVE-2019-0232	web服务器	可执行代码

Web 服务器（web 容器），包括：Tomcat、Apache、Ngnix

2、提供虚拟补丁功能，在不打补丁的情况下，可以防止攻击者利用机器现有的软件漏洞对软件发起攻击，还可对扫描出的软件漏洞进行标记修复、加白、

应用虚拟补丁等操作，提供虚拟补丁修复验证（复扫验证），可确认漏洞是否已成功修复，从而形成有效的漏洞闭环管理。

4.4.3 基线检查

基线检查可支持等级保护 2.0 的二级、三级检查、测评、整改的业务检查，系统内置官方等保 2.0 的二级、三级基线模板，以及应用未授权访问模板，还可支持用户自定义基线检查任务。并支持基线检查结果的图形化统计，包括：合规率、问题项 TOP5、风险服务器 TOP5 等维度的统计。覆盖 Ubuntu、Debian、CentOS、Windows Server 2008/2012/2016/2019，展现基线检测结果，报表中包含检查结果的所有数据，包括检查项信息，主机信息，检查结果，以及修复建议等，支持自定义检测模板。

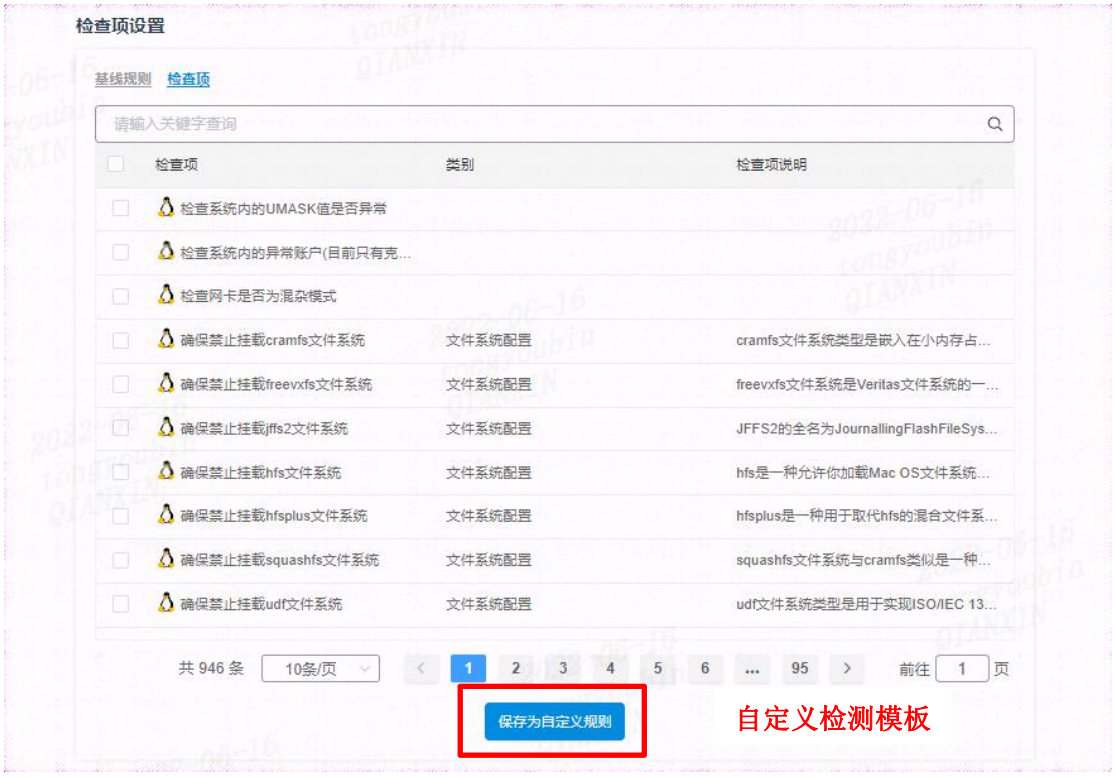
规则名称	
Windows Server 2019	查看 删除
Windows Server 2016	查看 删除
Windows Server 2012	查看 删除
Windows Server 2008	查看 删除
系统服务核查	查看
账户安全核查	查看
系统配置安全核查	查看
CIS_V2.2安全检查（Windows）	查看
CIS_V2.2安全检查（Linux）	查看

检查项

检查项名称	威胁等级	影响服务器	类别	操作
设置历史命令行数记录保证30条	超危	1	账号与登录设置	查看详情
以专门的用户帐号和组运行Apa...	超危	1	用户和组设置	查看详情
配置apache错误日志	超危	1	配置日志	查看详情
配置apache访问日志	超危	1	配置日志	查看详情
Tomcat密码复杂度判断	超危	1	身份鉴别	查看详情
Tomcat配置支持https加密协议	超危	1	身份鉴别	查看详情
禁止apache访问外部文件	高危	1	文件权限	查看详情
配置Apache错误页面重定向	高危	1	防攻击管理	查看详情
隐藏apache版本号及其它敏感...	高危	1	敏感信息泄露	查看详情
Tomcat更改默认端口	高危	1	防攻击管理	查看详情
Tomcat错误页面重定向	高危	1	防攻击管理	查看详情
配置apache日志记录格式	中危	1	配置日志	查看详情
更改apache默认端口	中危	1	防攻击管理	查看详情
禁止apache显示目录结构	超危	0	防攻击管理	查看详情
检查mysql是否配置日志功能	超危	0	配置日志	


设置历史命令行数记录保证30条
主机信息
请输入关键字查询
服务器名称
IPv4
AgentID
所属分组
检查结果
检查耗
centos
172.24.28.240,...
20de11b3201d...
123,业务,资...
不合规
1.0s
检查结果


检查项名称
服务器名称
IPv4
AgentID
所属分组
检查结果
设置历史命令行数记
centos
172.24.28.240,...
20de11b3201d...
123,业务,资...
不合规
设置历史命令行数记录保证30条
检查内容：30
检查结果：1000
处理意见（处理时请先做备份）
编辑/etc/profile: vim /etc/profile 设置 HISTSIZE=30, 执行命令：source /etc/profile 使其生效
修复建议
Tomcat配置支持http
禁止apache访问外


检查项设置
基线规则
检查项
请输入关键字查询
检查项
类别
检查项说明
检查系统内的UMASK值是否异常
检查系统内的异常账户(目前只有克...
检查网卡是否为混杂模式
确保禁止挂载cramfs文件系统
文件系统配置
cramfs文件系统类型是嵌入在小内存占...
确保禁止挂载freevxfs文件系统
文件系统配置
freevxfs文件系统是Veritas文件系统的一...
确保禁止挂载jffs2文件系统
文件系统配置
JFFS2的全名为JournallingFlashFileSys...
确保禁止挂载hfs文件系统
文件系统配置
hfs是一种允许你加载Mac OS文件系统...
确保禁止挂载hfsplus文件系统
文件系统配置
hfsplus是一种用于取代hfs的混合文件系...
确保禁止挂载squashfs文件系统
文件系统配置
squashfs文件系统与cramfs类似是一种...
确保禁止挂载udf文件系统
文件系统配置
udf文件系统类型是用于实现ISO/IEC 13...
共 946 条
10条/页
1
2
3
4
5
6
...
95
前往
1
页
保存为自定义规则
自定义检测模板

4.4.4 病毒查杀

病毒查杀支持本地、控制中心查杀两种方式进行病毒的查杀，支持本地查杀、控制中心查杀的设置与切换，内置 Bitdefender、ClamAV、Qowl 等多引擎技术识别并查杀最新病毒；同时并可对服务器的查杀规则进行详细设置，包括：实时防护的开启、文件夹、文件名查杀例外设置、勒索病毒防护（勒索诱饵防护、禁止删除系统还原点、内核免疫）、监控压缩包文件等设置。检测包含挖矿病毒、勒索病毒、内存病毒、内核病毒、木马、后门、蠕虫、钓鱼程序、黑客工具、漏洞利用代码、图片、宏文档等类型的恶意文件，可提供详细的恶意文件描述和解决方案，实时检查和主动扫描程序加载的 sh、py、ps1、vbs 等脚本的含恶意特征，实时监控无文件攻击行为，满足实时更新威胁情报库，实时检测恶意的 IP、域名、文件。


病毒详情
Js.Win32.CoinM
内核病毒
发现时间 2022-06-14
基本信息
检测说明
静态说明
检测描述
检测描述
通过文件实时监控，发现进程创建内核病毒 文件路径：/root/virus/b628e9be54adc342d0e569d4653f75cc。来源：病毒查杀


病毒详情
Trojan.Agent.e5ee83e5
发现时间 2022-06-13 10:22:11
基本信息
检测说明
静态说明
检测描述
检测描述
木马
通过文件实时监控，发现进程创建木马程序，文件路径：/root/virus/networkservice。来源：病毒查杀


病毒详情
Backdoor.Win32.Bladabindi.H
发现时间 2022-06-14 14:30:15
基本信息
检测说明
静态说明
检测描述
检测描述
后门
通过文件实时监控，发现进程创建后门程序，文件路径：/root/virus/1f48415da27265bf088d30b44efa80d5。来源：病毒查杀


病毒详情
Worm.Win32.Sytro.A
发现时间 2022-06-14 14:54:46
基本信息
检测说明
静态说明
检测描述
检测描述
蠕虫
通过文件实时监控，发现进程/usr/libexec/openssh/sftp-server创建蠕虫病毒，文件路径：/root/virus/3e1fd131851af609b536fe369ee86fe3。来源：病毒查杀


病毒详情
Worm.Win32.Sytro.A
发现时间 2022-06-14 14:54:46
基本信息
检测说明
静态说明
检测描述
检测描述
钓鱼程序
通过文件实时监控，发现进程/usr/libexec/openssh/sftp-server创建钓鱼程序 文件路径：/root/virus/3e1fd131851af609b536fe369ee86fe3。来源：病毒查杀


病毒详情
Worm.Win32.Sfone.B
发现时间 2022-06-14 14:54:45
基本信息
检测说明
静态说明
检测描述
检测描述
黑客工具
通过文件实时监控，发现进程/usr/libexec/openssh/sftp-server创建黑客工具文件路径：/root/virus/2df9de1b1b5c9b60d49bd3dd01c3cf82，来源：病毒查杀


病毒详情
Js.Win32.CoinMiner.H
发现时间 2022-06-14 15:19:28
基本信息
检测说明
静态说明
检测描述
检测描述
漏洞利用代码
通过文件实时监控，发现进程创建漏洞利用文件路径：/root/virus/4049aa5278f41ad298e562c10b5eb23e，来源：病毒查杀


病毒详情
Ransom.Win32.Agent.B
发现时间 2022-06-14 14:55:19
基本信息
检测说明
静态说明
检测描述
检测描述
图片
通过文件实时监控，发现进程创建图片文件路径：/root/virus/1d9093e8104d163ff3758e924b6e3606，来源：病毒查杀


病毒详情
Trojan.Agent.db5fef25
发现时间 2022-06-14 14:55:25
基本信息
检测说明
静态说明
检测描述
检测描述
宏文档
通过文件实时监控，发现进程创建宏文档文件路径：/root/virus/update.sh，来源：病毒查杀


病毒详情
Script.Win32.Webshell.UP
发现时间 2022-06-10 13:01:45
基本信息
检测说明
检测描述
恶意文件描述
检测描述
通过文件实时监控，发现进程/usr/libexec/openssh/sftp-server创建系统病毒，文件路径：/home/chyanxa/apache-tomcat-7.0.56/webapps/test.jsp，来源：病毒查杀


病毒处置
记录删除
白名单管理
更多...
加白
隔离
删除
解决方案
文件路径
感染服务器
服务器别名
操作系统
C:\nc\nc.exe
WIN2K8
Microsoft Windows S...
C:\nc.zip
WIN2K8
Microsoft Windows S...
/home/chyanxa/apac...
centos
CentOS Linux releas...
/root/xxx.jsp
/root/.cache/vmware/...


脚本路径: C:\Tfileless\Mimikatz.sh
文件类型: sh
文件大小: 2206859
文件访问权限: 32
文件MD5: f0f4bc53d852e0647dd7efd6d03386e2
文件所属用户: Administrators
文件所属用户组: BUILTIN
最近访问时间: 2022-02-14 14:57:41
创建时间: 2022-02-14 14:57:41
修改时间: 2021-08-21 16:12:27

SH


脚本路径: C:\Tfileless\Mimikatz. py
文件类型: py
文件大小: 2206859
文件访问权限: 32
文件MD5: f0f4bc53d852e0647dd7efd6d03386e2
文件所属用户: Administrators
文件所属用户组: BUILTIN
最近访问时间: 2022-02-14 14:57:41
创建时间: 2022-02-14 14:57:41
修改时间: 2021-08-21 16:12:27

PY


告警详情
powershell.exe
发生于: 2022-06-14 19:53:57
基本信息
静态说明
进程信息
动态说明
脚本路径: C:\Tfileless\Mimikatz.ps1
文件类型: ps1
文件大小: 2206859
文件访问权限: 32
文件MD5: f0f4bc53d852e0647dd7efd6d03386e2
文件所属用户: Administrators
文件所属用户组: BUILTIN
最近访问时间: 2022-02-14 14:57:41
创建时间: 2022-02-14 14:57:41
修改时间: 2021-08-21 16:12:27

PS1


脚本路径: C:\Tfileless\Mimikatz.vbs
文件类型: vbs
文件大小: 2206859
文件访问权限: 32
文件MD5: f0f4bc53d852e0647dd7efd6d03386e2
文件所属用户: Administrators
文件所属用户组: BUILTIN
最近访问时间: 2022-02-14 14:57:41
创建时间: 2022-02-14 14:57:41
修改时间: 2021-08-21 16:12:27

VBS

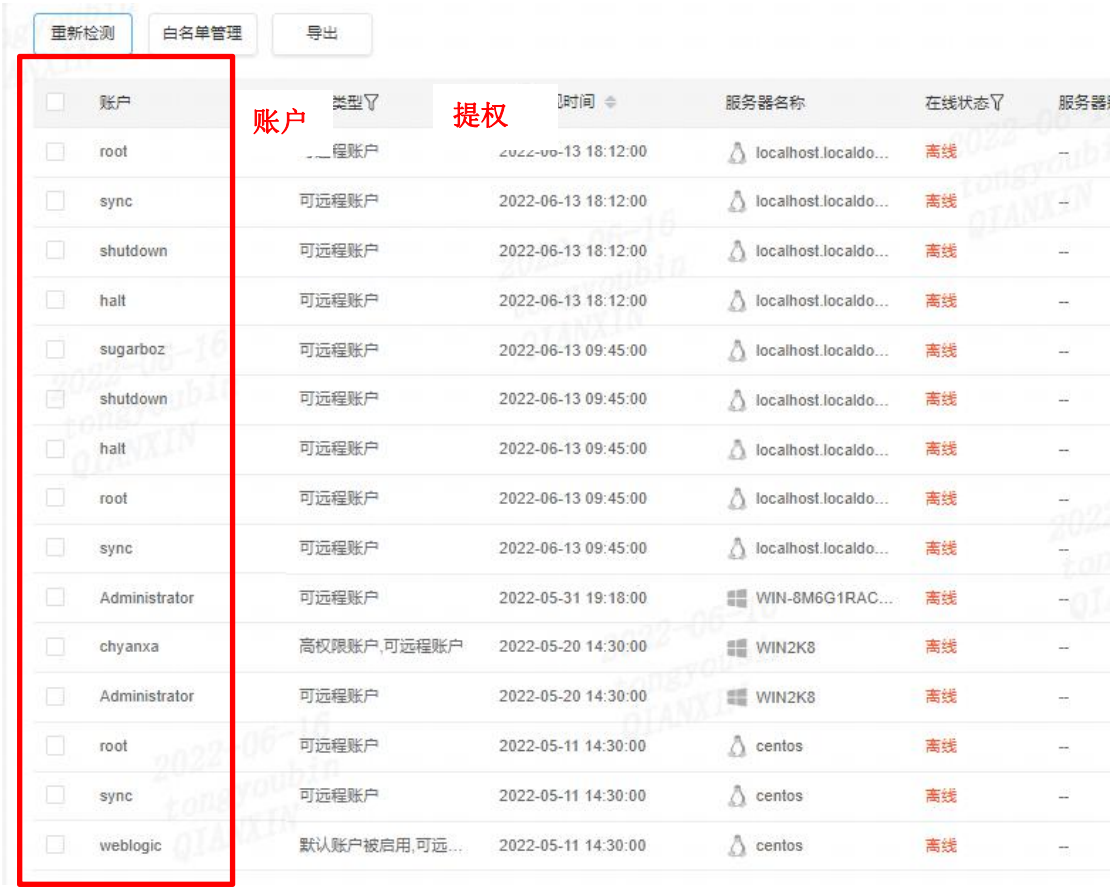

网神云锁 威胁监测 无文件攻击
告警列表
设置
白名单管理
导出
无文件攻击
发现时间 告警进程 告警类型 规则ID 规则描述 风险等级
2022-05-31 19:22:49 C:\WINDOWS\system3... 创建文件 34001 脚本文件创建 高危
2022-05-31 18:56:40 C:\Windows\System32\... 执行命令 30001 创建用户 危急
反连异常域名详情
危急
反连异常域名
发生于: 2021-10-28 17:28:55
基础信息 检测说明 动态信息 资产信息
实时更新威胁情报库
事件ID: 00fc0001
事件来源: 威胁监测>威胁情报
发生时间: 2021-10-28 17:28:55
事件等级: 危急
威胁类型: 威胁情报
已读状态: 未读
事件描述: 服务器上进程外连的域名命中威胁情报库中标记为危险的域名，该服务器可能已失陷，请及时研判处置。
处置状态: 未处置
处理建议: 请及时对该外连进程进行研判处理
处置时间: --
攻击方
攻击IP: --
IP所属: --
被攻击方
受害IP: 192.168.5.100
防护状态: 未拦截
受害资产: WIN-CSJHM5H4N76
所属分组: red
操作系统: Microsoft Windows Server 2012 R2 Datacenter Edition 64-bit
责任人: --
加入白名单
导出
恶意 IP、域名
请输入关键字查询
外连类型 外连IP 外连域名 外连端口 外连IP归属 威胁情报
外连内网 10.249.23.41 shjt2-ops-data01.qi... 88 局域网 --

4.5 威胁监测

威胁监测以图形化的形式统计并展示服务器的可疑威胁及告警信息，对文件、进程、端口、账户、提权、命令执行、远程控制、网络连接、恶意域名请求等异常行为的检测，包括检测异常行为的发现时间、目标 IP 地址、目标端口、连接进程、进程路径、父进程、进程树等信息，检测异常行为相关的文件路径、文件修改时间等，提供语法、词法、沙箱、机器学习、深度学习等多引擎安全检测，统计信息包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势，以及具体的威胁事件列表，可对主机中的各类威胁进行实时监测及处置，包括暴力破解、异常登陆、后门检测、反弹 shell、本地提权、Webshell、无文件攻击等威胁的监测与告警。

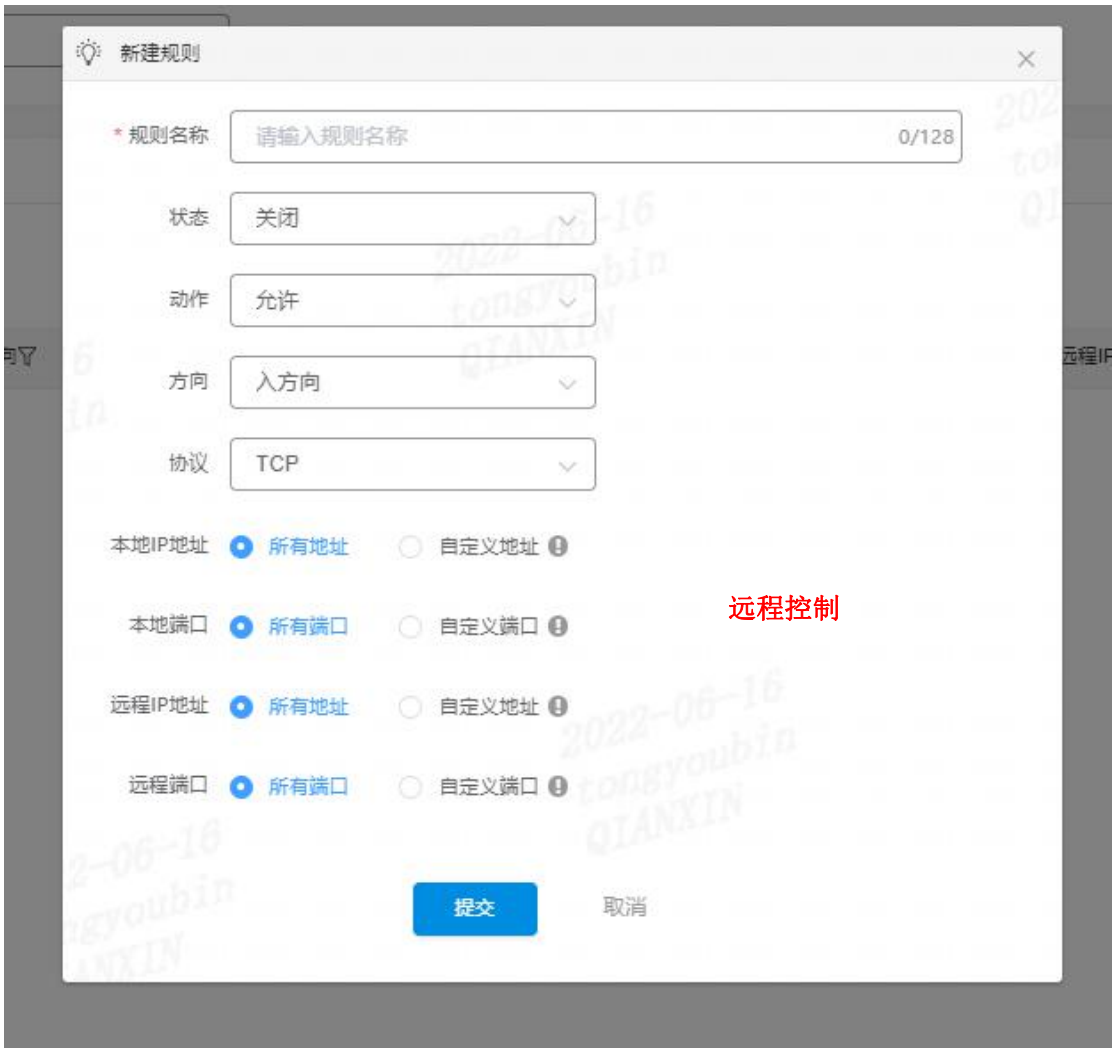
服务器名称	进程名称	服务器别名	AgentID	IPv4	IPv6	操作系统	所属分组	进程路径
WIN2K8	hydra.exe New		b07133c5189ee14a0...	172.24.28.134	fe80:00:00:00:8946:d...	Microsoft Wind...	123,业务	C:\hydra-8.1-window...
centos	go New		i201dac159...	172.24.28.253,127.0....	fe80::7c7d:e1dc:82a0...	CentOS Linux r...	123,业务	/usr/local/go/bin/go
localhost.localdo...	urlgrabber-ext-d...		a66a02cb0...	192.168.248.132,127...	fe80::3b2:cf48:56a1:...	CentOS Linux r...		/usr/libexec/urlgrabbe...
localhost.localdo...	yum New		29f18239a66a02cb0...	192.168.248.132,127...	fe80::3b2:cf48:56a1:...	CentOS Linux r...		/usr/bin/yum
centos	curl		20de11b3201dac159...	172.24.28.253,127.0....	fe80::7c7d:e1dc:82a0...	CentOS Linux r...	123,业务	/usr/bin/curl
centos	yum New		20de11b3201dac159...	172.24.28.253,127.0....	fe80::7c7d:e1dc:82a0...	CentOS Linux r...	123,业务	/usr/bin/yum
localhost.localdo...	gnome-softwar...		cbdc3fddfaa418cdf20...	172.24.28.233,127.0....	fe80::1905:a6c9:768...	CentOS Linux r...		/usr/bin/gnome-softw...
localhost.localdo...	yumBackend.py...		cbdc3fddfaa418cdf20...	172.24.28.233,127.0....	fe80::1905:a6c9:768...	CentOS Linux r...		/usr/share/PackageKi...
localhost.localdo...	geoclue New		cbdc3fddfaa418cdf20...	172.24.28.233,127.0....	fe80::1905:a6c9:768...	CentOS Linux r...		/usr/libexec/geoclue
USER-G0HVO...	System New		1669c7cd913eab16e...	172.24.28.249	fe80:00:00:00:3135:f...	Microsoft Wind...	业务	System
WIN2K8	spoolsv.exe		b07133c5189ee14a0...	172.24.28.134	fe80:00:00:00:8946:d...	Microsoft Wind...	123,业务	C:\windows\system3...

服务器名称	端口号	服务器别名	操作系统	AgentID	IPv4	IPv6	所属分组
localhost.localdo...	22 New		CentOS Linux r...	acb70de0a8df91474...	192.168.137.100,127...	fe80::215:5dff:fe03:6...	
localhost.localdo...	22 New		CentOS Linux r...	29f18239a66a02cb0...	192.168.248.132,127...	fe80::3b2:cf48:56a1:...	
localhost.localdo...	8080 New		CentOS Linux r...	cbdc3fddfaa418cdf20...	172.24.28.233,127.0....	fe80::1905:a6c9:768...	
WIN2K8	8080		Microsoft Wind...	b07133c5189ee14a0...	172.24.28.134	fe80:00:00:00:8946:d...	123,业务
WIN2K8	49152 New		Microsoft Wind...	b07133c5189ee14a0...	172.24.28.134	fe80:00:00:00:8946:d...	123,业务
WIN2K8	49155 New		Microsoft Wind...	b07133c5189ee14a0...	172.24.28.134	fe80:00:00:00:8946:d...	123,业务
WIN2K8	139 New		Microsoft Wind...	b07133c5189ee14a0...	172.24.28.134	fe80:00:00:00:8946:d...	123,业务
WIN2K8	7001		Microsoft Wind...	b07133c5189ee14a0...	172.24.28.134	fe80:00:00:00:8946:d...	123,业务
WIN2K8	445 New		Microsoft Wind...	b07133c5189ee14a0...	172.24.28.134	fe80:00:00:00:8946:d...	123,业务
USER-G0HVO1...	49152 New		Microsoft Wind...	1669c7cd913eab16e...	172.24.28.249	fe80:00:00:00:3135:f...	业务
USER-G0HVO1...	139 New		Microsoft Wind...	1669c7cd913eab16e...	172.24.28.249	fe80:00:00:00:3135:f...	业务
USER-G0HVO1...	49155 New		Microsoft Wind...	1669c7cd913eab16e...	172.24.28.249	fe80:00:00:00:3135:f...	业务
USER-G0HVO1...	445 New		Microsoft Wind...	1669c7cd913eab16e...	172.24.28.249	fe80:00:00:00:3135:f...	业务
localhost.localdo...	22 New		CentOS Linux r...	cbdc3fddfaa418cdf20...	172.24.28.233,127.0....	fe80::1905:a6c9:768...	
centos	8080		CentOS Linux r...	20de11b3201dac159...	172.24.28.253,127.0....	fe80::7c7d:e1dc:82a0...	123,业务


重新检测
白名单管理
导出
账户
提权
账户
类型
时间
服务器名称
在线状态
root 可远程账户 2022-06-13 18:12:00 localhost.localdo... 离线
sync 可远程账户 2022-06-13 18:12:00 localhost.localdo... 离线
shutdown 可远程账户 2022-06-13 18:12:00 localhost.localdo... 离线
halt 可远程账户 2022-06-13 18:12:00 localhost.localdo... 离线
sugarboz 可远程账户 2022-06-13 09:45:00 localhost.localdo... 离线
shutdown 可远程账户 2022-06-13 09:45:00 localhost.localdo... 离线
halt 可远程账户 2022-06-13 09:45:00 localhost.localdo... 离线
root 可远程账户 2022-06-13 09:45:00 localhost.localdo... 离线
sync 可远程账户 2022-06-13 09:45:00 localhost.localdo... 离线
Administrator 可远程账户 2022-05-31 19:18:00 WIN-8M6G1RAC... 离线
chyanxa 高权限账户,可远程账户 2022-05-20 14:30:00 WIN2K8 离线
Administrator 可远程账户 2022-05-20 14:30:00 WIN2K8 离线
root 可远程账户 2022-05-11 14:30:00 centos 离线
sync 可远程账户 2022-05-11 14:30:00 centos 离线
weblogic 默认账户被启用,可远... 2022-05-11 14:30:00 centos 离线


本地提权详情
被提权主机 :172.24.28.190
发生于: 2022-05-06 13:31:24
进程信息
进程树
进程名: bash
运行用户: root
提权进程路径: /usr/bin/bash
用户组: root
完整文件权限: rwxr-xr-x
父进程名: su
运行用户: weblogic
提权进程路径: /usr/bin/su
用户组: root


RCE告警详情
RCE利用
发生于：2022-06-08 18:39:29
基础信息
检测说明
动态信息
进程树
发现时间：2022-06-08 18:39:29
主机IP：172.24.28.253
服务名：
端口号：7001
服务器名：centos
AgentID：20de11b3201dac159be154c80bd6414e
服务路径：/usr/java/jdk1.7.0_80/bin/java
执行命令：/usr/bin/whoami
命令执行


新建规则
* 规则名称
请输入规则名称
0/128
状态
关闭
动作
允许
方向
入方向
协议
TCP
本地IP地址
所有地址
自定义地址
本地端口
所有端口
自定义端口
远程IP地址
所有地址
自定义地址
远程端口
所有端口
自定义端口
提交
取消
远程控制


加入白名单
导出
删除
请输入关键字查询
外连类型
外连IP
外连域名
外连端口
外连IP归属
威胁情报
外连内网 10.249.23.41 shjt2-ops-data01.qi... 88 局域网 --
外连内网 10.249.23.41 shjt2-ops-data01.qi... 389 局域网 --
外连内网 10.46.21.107 zzbm-ops-data02.qi... 389 局域网 --
网络连接
共 3 条
1


服务器jowto18v.center.bjzt.qianxin-inc.cn进程/usr/libexec/sssd/sssd_be的外连详情
加入白名单
导出
删除
请输入关键字查询
恶意域名请求
外连类型
外连IP
外连域名
外连端口
外连IP归属
威胁情报
外连内网 10.249.23.41 shjt2-ops-data01.qi... 88 局域网 --
外连内网 10.249.23.41 shjt2-ops-data01.qi... 389 局域网 --
外连内网 10.46.21.107 zzbm-ops-data02.qi... 389 局域网 --
共 3 条
1

基础信息 检测说明 资产信息

事件详情

事件ID：000e0000
发生时间：2022-06-14 14:47:25
威胁类型：账户异常
事件描述：登录服务器账户不是常用账号，或者不在常用登录地区登录。如非本人登录，则异地登录意味着服务器密码已泄露或被破解，已被他人成功登入服务器。
处理建议：该类事件的报警，说明服务器密码已经被获取且被恶意用户成功登录服务器。建议修改服务器远程登录端口，并修改登录密码为复杂密码。同时开启云中心登录防护，限制登录时间、登录IP及远程登录的计算机名。

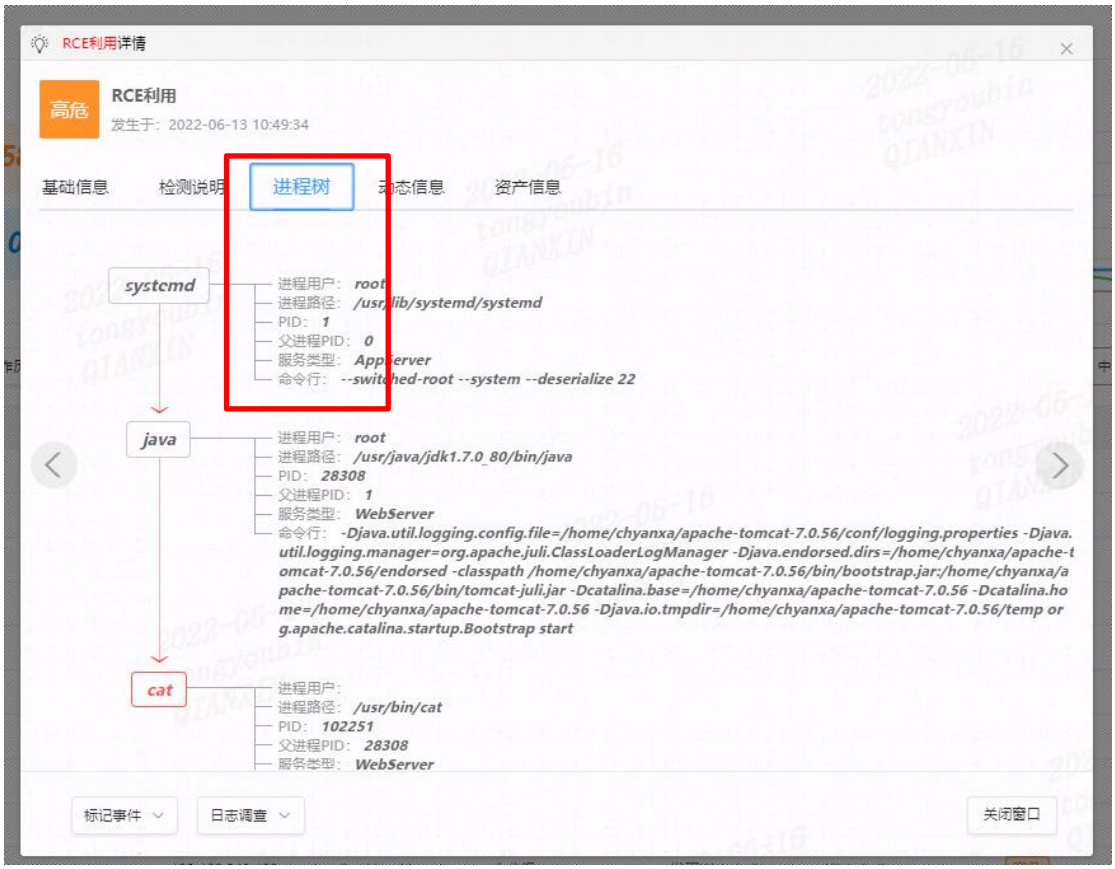
发现时间

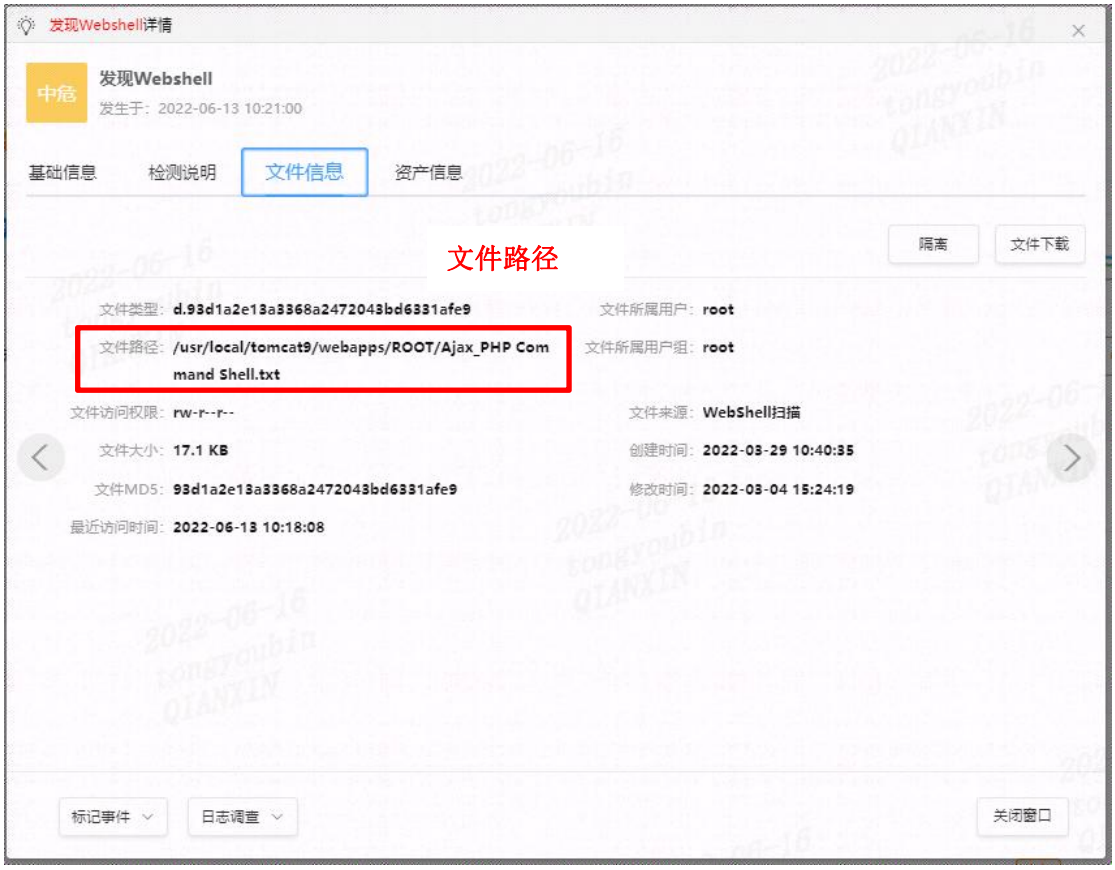
事件来源：威胁监测>异常登录
事件等级：中危
已读状态：未读
处置状态：
处置时间：--

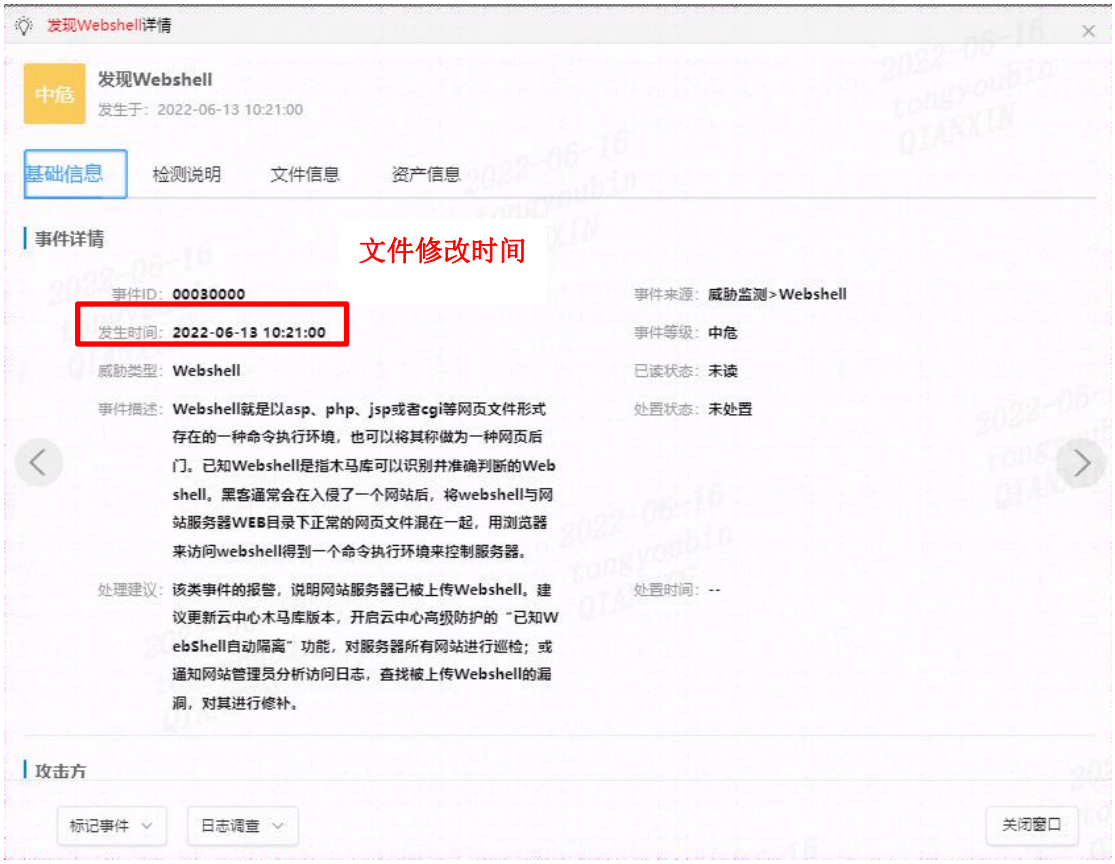
攻击方

攻击IP：172.24.28.1
IP所属：局域网

目标 IP、目标端口


RCE利用详情
高危
RCE利用
发生于：2022-06-13 10:49:34
基础信息
检测说明
进程树
动态信息
资产信息
systemd
进程用户：root
进程路径：/usr/lib/systemd/systemd
PID：1
父进程PID：0
服务类型：AppServer
命令行：--switched-root --system --deserialize 22
java
进程用户：root
进程路径：/usr/java/jdk1.7.0_80/bin/java
PID：28308
父进程PID：1
服务类型：WebServer
命令行：-Djava.util.logging.config.file=/home/chyanxa/apache-tomcat-7.0.56/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.endorsed.dirs=/home/chyanxa/apache-tomcat-7.0.56/endorsed -classpath /home/chyanxa/apache-tomcat-7.0.56/bin/bootstrap.jar:/home/chyanxa/apache-tomcat-7.0.56/bin/tomcat-juli.jar -Dcatalina.base=/home/chyanxa/apache-tomcat-7.0.56 -Dcatalina.home=/home/chyanxa/apache-tomcat-7.0.56 -Djava.io.tmpdir=/home/chyanxa/apache-tomcat-7.0.56/temp org.apache.catalina.startup.Bootstrap start
cat
进程用户：
进程路径：/usr/bin/cat
PID：102251
父进程PID：28308
服务类型：WebServer
标记事件
日志调查
关闭窗口

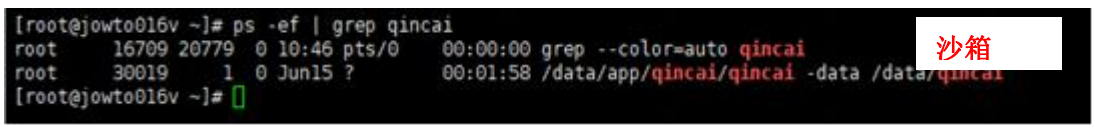

发现Webshell详情
中危
发现Webshell
发生于：2022-06-13 10:21:00
基础信息
检测说明
文件信息
资产信息
文件路径
隔离
文件下载
文件类型：d.93d1a2e13a3368a2472043bd6331afe9
文件所属用户：root
文件路径：/usr/local/tomcat9/webapps/ROOT/Ajax_PHP Command Shell.txt
文件所属用户组：root
文件访问权限：rw-r--r--
文件来源：WebShell扫描
文件大小：17.1 KB
创建时间：2022-03-29 10:40:35
文件MD5：93d1a2e13a3368a2472043bd6331afe9
修改时间：2022-03-04 15:24:19
最近访问时间：2022-06-13 10:18:08
标记事件
日志调查
关闭窗口



类型	关键字	描述
	object.cmdline	命令行参数
	object.src	源地址
	object.dst	目标地址
	object.other	其他客体
登录日志相关参数	login.pcName	远程登录PC名
	login.loginUser	远程登录用户
其他参数	typeName	日志类型
	result	拦截结果0：已拦截，1：未拦截
	attId	ATT&CK_ID
	tactics	ATT&CK攻击阶段（策略）
	categoryName	日志分类名称，如:网络行为日志,进程操作日志,文件操作日志
逻辑符号	&&	与

语法、词法

关闭



4.5.1 威胁总览

威胁总览以图形化的形式，统计并展示服务器的可疑威胁及告警信息，识别和阻断入侵开始阶段的端口映射、端口转发、内网代理等隧道代理搭建行为。识别和阻断入侵持久化阶段的反弹 shell、远程控制等行为，识别和阻断入侵收尾阶段的数据清除行为，汇总信息包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势，以及具体的威胁事件列表，并可对威胁事件进行研判，还可将威胁事件导出为 EXCEL 格式的报告。


服务器jowto18v.center.bjzt.qianxin-inc.cn进程/data/app/qincai/qinc 端口7901的暴露详情
端口转发
加入白名单
导出
删除
请输入关键字查询
暴露类型 目标IP 源IP IP归属 威胁情报 备注 首次暴露时间
内网暴露 10.47.140.55 10.44.11.147 局域网 -- 请输入备注 2022-06-15 22:34:53
内网暴露 10.47.140.55 10.95.58.114 局域网 -- 请输入备注 2022-06-14 04:15:05
内网暴露 10.47.140.55 10.95.58.136 局域网 -- 请输入备注 2022-06-12 10:57:45


中危
代理隧道
发生于：2022-05-31 17:03:21
隧道代理
基础信息
检测说明
文件信息
动态信息
资产信息
事件详情
事件ID：001d0003
发生时间：2022-05-31 17:03:21
威胁类型：代理隧道程序
事件描述：发现代理隧道程序，请及时研判处置。
处理建议：--
事件来源：威胁监测>代理隧道
事件等级：中危
已读状态：未读
处置状态：未处置
处置时间：--


网神云锁 威胁监测 反弹shell
反弹 shell
批量操作
白名单规则
告警设置
导出
发现时间 发起连接主机 服务器名称 服务器别名 AgentID
2022-05-31 18:02:08 172.24.28.226 centos -- 20de11b3201da...
2022-05-23 11:01:03 172.24.28.189 172.24.28.189 -- cbdc3fddfaa418...
2022-05-23 10:58:59 172.24.28.189 172.24.28.189 -- cbdc3fddfaa418...
2022-05-23 10:56:58 172.24.28.189 172.24.28.189 -- cbdc3fddfaa418...
2022-05-23 10:56:57 172.24.28.189 172.24.28.189 -- cbdc3fddfaa418...
2022-05-06 13:29:39 172.24.28.190 centos -- 20de11b3201da...

4.5.2 恶意扫描

恶意扫描可自动识别端口扫描行为及扫描器并进行威胁告警，还可防止漏洞扫描并屏蔽扫描器，并将监测到的攻击信息以列表的形式进行展示，并可导出 EXCEL 格式的文件。

4.5.3 暴力破解

暴力破解入侵检测功能用于检测发现主机上各类关键应用被尝试登录的行为，防止登录账户被爆破。能够在检测到爆破行为时生成暴力破解入侵记录，同时给用户提供根据封禁配置自动或手动封停爆破来源 IP 的能力，展示暴力破解影响的资产信息、攻击源 IP 地址、服务类型、攻击时间、事件状态、事件处理记录等信息。

4.5.4 异常登陆

异常登录功能实时监控主机上发生的异常登录行为，包括非常用时间登录、非常用地点登录、非常用 IP 登录、非常用账号登录等异常登录，并发送邮件通知用户。用户可以在界面上查看这些异常登录事件，可通过设置正常登录规则判定哪些为正常的登录行为，正常登录外的行为被认为是异常登录行为。

4.5.5 后门检测

通过检测服务器上存在的二进制后门程序，发现服务器上的威胁，及时上报处置。包括三种检测方式、本地文件特征、程序命令行检测、已经运行的进程实时监控、可以对系统进行实时监测后门运行并进行告警。

4.5.6 Webshell

通过检测主机 Web 目录下的文件内容，发现 Web 网站中是否存在后门文件，并对发现的后门进行记录，并支持内存 Webshell 检测，提供实时监控方式来发现后门，并支持多种检测引擎。用户可以查看和处理发现的 Webshell，还能够查看 Webshell 的具体文件信息并下载后门文件。并支持速度优先、性能优先两种方式，可在高速扫描（高性能）/低速扫描（低功耗）之间进行选择，满足多种服务器扫描场景。

4.5.7 反弹 Shell

反弹 shell 用于监控主机中所有利用 Shell 进行反向连接的行为。当有反向连接发生时，系统生成反弹 shell 事件记录，用户可以查看并处理这些反弹事件。当反弹 shell 的目的 IP 为内网 IP 时，系统生成反弹 shell 记录并上报告警。

4.5.8 本地提权

当用户以低权限进入主机，通过某种行为获得高权限时，该进程很有可能是黑客的网络攻击行为。

4.5.9 无文件攻击

通过多种系列高危应用进行实时监控，发现服务器上的无文件攻击事件，及时上报处置。基于九种行为对系统进行检测，九种行为又对应不同的规则，包括命令执行、方法注入等方式的规则。

4.5.10 RCE 利用

RCE 利用基于行为分析，检测对外服务的远程命令执行漏洞利用行为，实现实时告警和追溯。

4.6 分析中心

当安全事件发生后，系统可自动回溯黑客攻击过程、提供攻击过程分析、生成事件分析报告，实现入侵取证。采用行为关联分析方法将访问行为过程中所产生的日志进行综合分析比对，将入侵行为分别以探测、攻击、控制、其他等阶段，并以安全事件的方式发出告警，实时监控记录恶意攻击发生的路径及关键点，利用监控所获取的数据，分析事件完整过程，找出根本原因。

4.7 Agent 管理

4.7.1 策略模板管理

Agent 策略模板管理可对服务器防护策略进行统一的管理、设置、下发，并基于不同的防护场景定制不同的策略，并将定制的策略模板统一下发到 Agent 服务器中。

4.7.1.1 应用防护策略

支持批量或单台机器开启应用防护策略。包括应用漏洞防护、虚拟补丁、高级防护、URL 控制等策略。检测包含且不限于 php、java、asp、jsp、jspx 等类型的 webshell 文件，可查看文件详情信息和下载文件。清点各类 Web 服务信息，至少包括：Apache、Nginx、Tomcat、Weblogic、WebSphere、IIS、Jboss、Wildfly、Jetty、HIS、Tegine，清点服务信息中应包含不仅限：服务名称，服务版本，启动用户，二进制文件路径等。

4.7.1.2 系统防护策略

支持批量或单台机器开启系统防护策略，系统防护包括文件监控与防护、操作系统加固。

4.7.1.3 网络防护策略

支持批量或单台机器开启网络防护策略。包括防端口扫描、IP 黑白名单等策略。

4.7.1.4 全局策略开关

支持批量或单台机器开启防护开关、批量设置卸载密码、批量设置自身防护等策略。支持邮件、短信、站内信形式的告警通知。


用户信息
邮件告警
* 用户名称
请输入用户名称
0/50
* 邮箱
请输入邮箱
* 账户密码
请输入账户密码
服务器信息
* 发送邮件服务器
请输入发送邮件服务器
0/50
* 端口号
请输入端口号
使用NTLM验证
使用ssl连接服务器
发送测试邮件


序号
通知对象
操作
1
test_1
序号
状态
告警状态
通知条件
通知方式
操作
1
告警发生时
任何时间/提醒告警/立刻
短信告警
2
告警发生时
任何时间/提醒告警/立刻
3
告警发生时
任何时间/提醒告警/立刻


站内信
站内信告警
+新建
全部
未读
已读
已发送
草稿
关键字
序号 发件人 收件人 时间 标题 内容 级别 状态
1 超级管理 超级管理 2017-04-17 13:41:17 test test 高 已读
2 超级管理 超级管理 2017-04-16 17:46:18 测试标题 测试内容 普通 已读
3 超级管理 超级管理 2017-04-12 16:10:27 消息 是多少 普通 已读
4 超级管理 超级管理 2017-04-12 16:00:09 你好，我是管理员，现在测试站内信 你好，我是管理员，现在测试站内信 普通 已读
5 超级管理 超级管理 2017-04-12 14:00:23 测试邮件 测试邮件 普通 已读
显示 1/1 页，共 5 条

4.7.2 策略下发管理

支持将定制的策略模板，进行批量下发，并对下发的状态进行监控。

4.7.3 Agent 更新管理

4.7.3.1 Agent 安装情况看板

以图表的形式，对 Agent 的安装情况进行实时监控，包括：Agent 版本分布、可升级版本占比等信息，并以列表的形式列出服务器中安装的 Agent 详细信息。

4.7.3.2 Agent 安装同步

可对 Agent 的安装情况进行实时同步，包括：服务器名称、所属分组、Agent 安装时间、当前 Agent 版本、最新 Agent 版本、Agent 类型、启动时间、结束时间、更新状态等信息。

4.8 服务器性能监控

可显示当前所有服务器的 CPU、内存、硬盘使用情况，包括内存使用率、硬盘空间、操作系统、agent 利用率等等信息，并提供报警和导出功能

4.9 子账号管理

支持子账号管理，并可设置某账号管理不同的机器，支持账号名称、账号角色、上级账户关联、归属人、手机号、邮箱、备注等信息的设置。

5 客户价值

5.1 不改变企业现有的系统及应用

奇安信网神云锁服务器安全管理系统，不会更改原有的业务流程，对系统和应用完全透明，系统和应用性能无影响。

5.2 提升安全运维效率

奇安信网神云锁服务器安全管理系统帮助企业减少安全风险，使运维人员提升安全运维效率，减少安全事件的发生概率，提升业务系统正常运行的安全性、可靠性、稳定性，减少企业的安全风险。减少企业人力成本投入。同时保护了业务连续性和数据安全。

5.3 动态的安全防御体系

依靠 AI 智能学习能力动态更新安全防护策略辨识用户进程操作行为，结合大数据情报挖掘、精准定位安全风险，打破传统的需要投入大量人力实时监控，频繁修复漏洞、升级补丁的，以及以部分业务牺牲为代价的安全防护模式。从被动的频发被外界攻击、处理安全事件工单，疲于应付，转型主动防御，自适应网络安全架构，动态调整安全防护策略，从而形成动态安全防御体系。

6 应用场景

产品可用于等保合规，勒索挖矿防治，防暴露、防扫描，微隔离，0Day 防护等场景。

6.1 等保合规场景

可对服务器的资产信息进行全面盘点，覆盖 15 个维度，同时覆盖等保 2.0 中二级、三级 560 余项基线检查项，并支持病毒查杀与防勒索等场景。同时基于微隔离白名单机制、漏洞扫描、弱口令、防爆破、WebShell、安全日志等手段进行综合联防联控。

图 11 等保合规场景

6.2 勒索挖矿防治场景

云锁基于防勒索挖矿的最佳实践，并结合自主研发的 Qowl 杀毒引擎，解决了传统服务器杀毒无法对中毒机器隔离的问题。

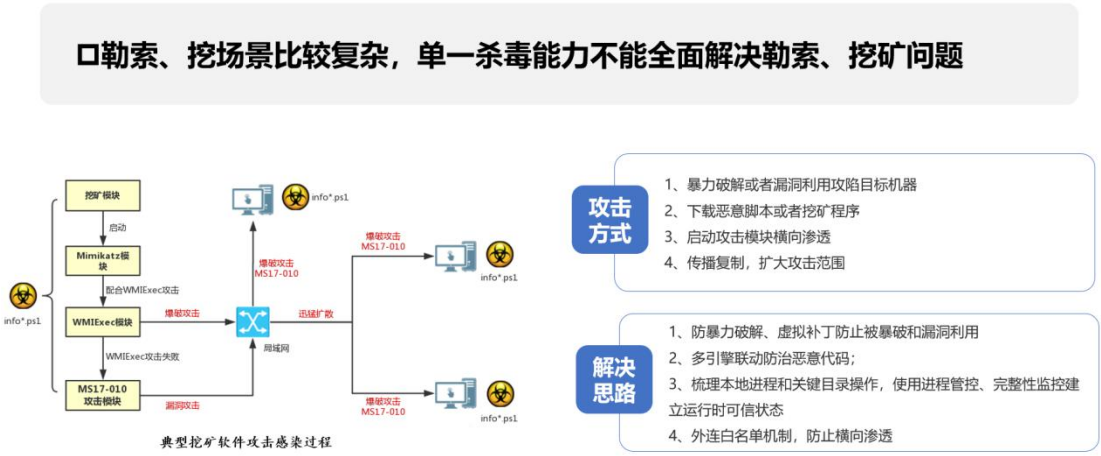


图 12 防勒索挖矿场景

6.3 防暴露、防扫描场景

云锁采用资产探测和暴露面技术，并结合端口防扫描技术，不但能对黑客的端口扫描进行告警、拦截，还可对端口扫描进行扫描者溯源，还可防止漏扫工具对服务器进行弱点和漏洞扫描。

图 13 防暴露、防扫描场景

6.4 微隔离防入侵、防扩散

云锁基于端口白名单信任域、外连白名单信任域，真正实现服务器间的微隔离，彻底切断外连攻击、横向渗透。

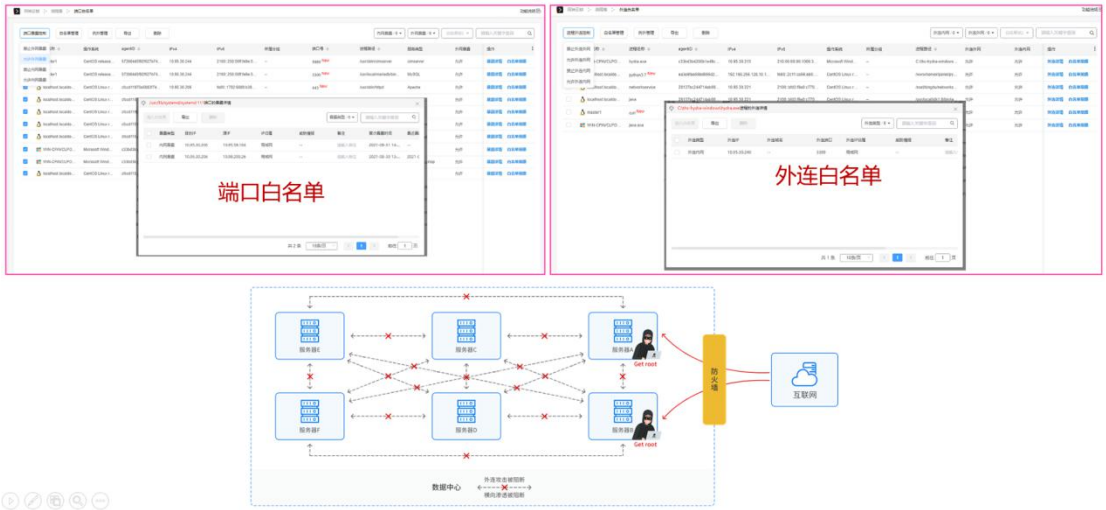


图 14 微隔离场景

6.5 0DAY 防护场景

云锁结合异常行为分析、外连白名单管控，以及攻击路径溯源等能力，实现对 0DAY 攻击的先知、先决。

图 15 ODAY 防护场景

7 安装部署

7.1 部署架构

系统管理控制中心与 agent 均可直接部署在物理机/虚拟机中，管理中心可单节点部署也支持分布式部署。产品部署架构如下图所示：

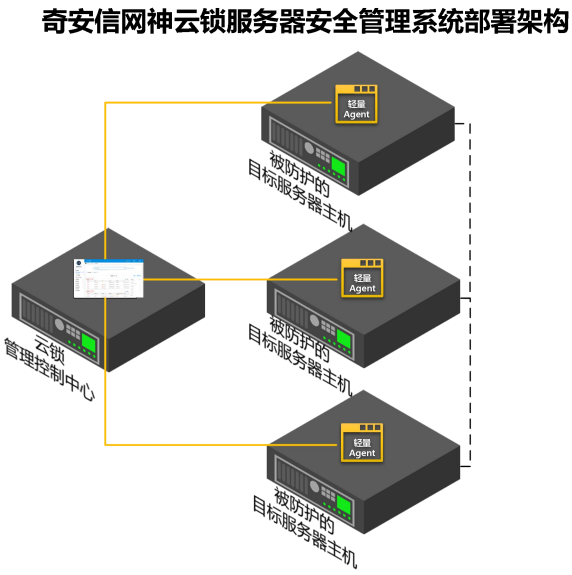


图 16 系统部署架构

7.2 硬件配置要求

注：配置要求场景：按管理控制中心 180 天日志留存要求，每台客户端开启全量日志记录的情况下，服务端及客户端配置如下表所示，且探针数量支持扩展：

服务端/客户端	类别	客户端数量	部署模式	CPU 资源	内存资源	硬盘资源	备注
服务端	管理控制中心	100 点及以下	单节点	16 核	32G	500G 剩余空间	为保障云锁在不同客户场景下的性能高并发 5000Agent 客户端以上的管理中心服务端硬件需定制，详情见表 2
		100~200 点	单节点	32 核	64G		
		200~500 点	单节点	64 核	128G		
		500~1000 点	3 节点	32 核/节点	64G/节点	1T/节点	
		1000~2000 点	5 节点	32 核/节点	64G/节点		
		2000 ~ 3000 点	7 节点	32 核/节点	64G/节点		
		3000 ~ 5000 点	9 节点	32 核/节点	64G/节点		
		5000 ~ 10000 点	11 节点	/	/	/	
		10000 ~ 15000 点	13 节点	/	/		
客户端	Agent 客户端	按需配置	--------	2 核	4G	5G 剩余空间	

表 2：

5000Agent 客户端以上的服务器硬件配置要求	
CPU	2*X86CPU≥10 核或 2*ARM 架构 CPU≥32 核
频率	主频≥2.1GHz
内存	内存≥128GB
存储	系统盘单盘容量≥960GB 的 3 块 SATA SSD 盘，数据盘单盘容量≥1.8TB 10K(转数)的 6 块 SAS 盘，满足 RAID 0/1/5/6
缓存	缓存≥2GB
机箱尺寸	2U
电源	双电源
网卡	千兆网卡≥2
网络接口	每块网卡≥2 个千兆电口，≥2 个万兆网卡，每块网卡≥2 个万兆光口，实配 SFP 模块
机箱尺寸	2U

7.3 操作系统支持

以下为管理控制中心、Agent 客户端支持的操作系统列表，因管理控制中心的操作系统要求为 X64 CentOS7.0 以上，如客户侧只能使用其他版本的操作系统，请向二线确认。

服务端/客户端	类别	CPU 架构	操作系统版本及内核要求
服务端	管理控制中心	X86/X64	CentOS 7.0 X64
客户端	Agent 客户端		Windows Server 2003 sp2/R2 x86/x64
			Windows Server 2008 sp1 及以上/R2 x86/x64
			Windows Server 2012~2019 sp1 及以上/R2 x86/x64
			CentOs 5.0 及以上 x86/x64
			RHEL 5.5 及以上
			Ubuntu 14.04 及以上 x86/x64
			SUSE 11 及以上版本 x86/x64
		ARM	Kylin Linux 4.18.0-147 及以上
			Deepin-4.19.0-arm64-server_1707/1813