八分量持续免疫系统

技术白皮书

版本编号：v1.0

2020年03月20日

版本记录

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 日期 | 作者 | 修订说明 |
| v.1.0 | 2020-03-20 | 八分量产品部 | 初稿 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1 系统概述 2](#_Toc36579284)

[1.1 摘要 2](#_Toc36579285)

[1.2 威胁层出不穷 2](#_Toc36579286)

[1.3 名词解释 3](#_Toc36579287)

[2 八分量持续免疫系统设计方案 4](#_Toc36579288)

[2.1 持续免疫系统的设计理念 5](#_Toc36579289)

[2.2 持续免疫系统架构介绍 5](#_Toc36579290)

[3 产品特点 12](#_Toc36579291)

[4 产品功能 13](#_Toc36579292)

[4.1 可信防护 13](#_Toc36579293)

[4.2 用户行为分析 14](#_Toc36579294)

[4.3 主动对抗 15](#_Toc36579295)

[4.4 区块链防篡改 16](#_Toc36579296)

[4.5 功能介绍 17](#_Toc36579297)

[5 产品运维部署 25](#_Toc36579298)

[5.1 SaaS部署 25](#_Toc36579299)

[5.2 私有网物理隔离部署 25](#_Toc36579300)

[5.3 组件式布署 26](#_Toc36579301)

[5.4 批量部署与SMDB兼容 26](#_Toc36579302)

[5.5 持续免疫系统运维架构 27](#_Toc36579303)

[5.6 运维分组结构 28](#_Toc36579304)

[5.7 运维展示管控中心 28](#_Toc36579305)

[5.8 区域可信证实服务运维服务 29](#_Toc36579306)

[6 安装及配置环境与性能规格说明 30](#_Toc36579307)

[6.1 环境要求 30](#_Toc36579308)

[6.2 安装主机脚本分布概况举例 30](#_Toc36579309)

[6.3 服务端配置和性能指标 31](#_Toc36579310)

[6.4 可信证实配置和性能指标 31](#_Toc36579311)

[7 产品优势 33](#_Toc36579312)

1. 系统概述

* 1. 摘要

如今全球化、远程化和移动化办公员工与日俱增，面对这一形势，企业必须在安全的内部网络中创建更多的入口点，才能确保关键系统的可访问性。这一转变引发了新需求，即要求放松严格的网络访问和防火墙规则，或利用更常用的网络协议访问这些系统上的数据，从而找到规避这些限制的方法。在这些形势共同作用下，强化端点自身的需求日益高涨，仅靠边界安全来确保关键系统的安全性已经捉襟见肘。

八分量持续免疫系统解决方案通过在重要的客户端和服务器上强制实施基于行为的安全策略，可以抵御零日攻击、强化系统并保持遵从。

* 1. 威胁层出不穷

随着商业软件漏洞数量与日俱增，而利用这些漏洞发起攻击的时间却日渐缩短，企业继续成为重点攻击目标。企业忙于在攻击者利用漏洞发起攻击之前修补其关键系统，这是一项劳民伤财的工作。

计算机紧急情况应对小组 (CERT®) 和八分量安全响应中心的最新研究表明，随着发动攻击的动机从追求名气转变为追求经济利益，攻击者和威胁日趋复杂，威胁的生命周期越来越短，并且在不断探索新的攻击媒介来危害系统。

自1988年出现首例互联网蠕虫以来，技术和信息安全已经取得了长足发展，但是网络和主机面临的威胁却一如既往。与当今的威胁非常类似，这种“蠕虫”利用连接到互联网的计算机上存在的软件漏洞，这个漏洞往往需要花费很长时间才能加以识别和修补。如今，我们依赖各种系统来存储和检索数据、与客户和合作伙伴进行通信以及开展业务交易，这些系统仍然遭受相同的漏洞威胁。如此看来，当今系统的安全性甚至不及1988年。2017年后互联世界再次屈服于另一个威胁 – 勒索病毒，其能够利用已知但未修复的漏洞，自动像蠕虫一样传播和攻击。

这些威胁揭示了这样的事实：攻击者正在利用容易利用的漏洞，有时是公开的漏洞。那些对编码知识要求不高，甚至无需编码知识即可利用的漏洞数量与日俱增，而利用漏洞发起攻击的时间却越来越短。

* 1. 名词解释

|  |  |
| --- | --- |
| 缩略语 | 描述 |
| UEBA | 大数据用户行为画像分析，是通过人工智能对用户的行为进行聚合画像的功能。 |
| POC | 即Proof of Concept，是业界流行的针对客户具体应用的验证性测试。 |
| TPM | 可信赖平台模块，TPM标准由可信赖计算组织 |
| 0day漏洞 | 安全补丁发布前而被了解和掌握的漏洞信息。 |
| RPC | 远程过程调用, 是一种通过网络从远程计算机程序上请求服务。 |
| TCM | Trusted Cryptography Module，我国自主研发的可信安全芯片 |
| OAT | 证实服务 |
| NISA | 用户行为分析引擎。 |
| SVN | 一个开放源代码的版本控制系统。 |
| SNORT | 一款开源入侵检测系统。 |
| SNMP TRAP | 是一种标准的报告机制,广泛应用在各种网络管理软件中。 |
| GIT | 是一个开源的分布式版本控制系统,用于敏捷高效地处理任何或小或大的项目。 |
| WAF | 网站应用级入侵防御系统。 |

1. 八分量持续免疫系统设计方案

未知威胁层出不穷、0day 攻击难以防范、监管追责日趋严厉的信息化新趋势下，服务器数据存储面临着数据库注入攻击、文件管理混乱、行为记录缺损等数据风险。一旦数据泄露发生，将给企业和民众造成无法估量的损失。面对已经攻入系统的入侵者，如何能快速发现并处置，进而保障业务的安全稳定，同时行为记录可追踪？

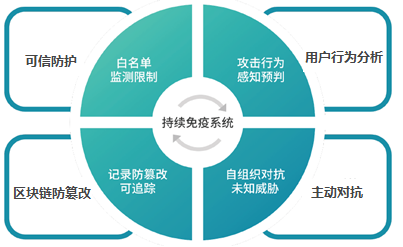


图2-1

八分量团队开创性地提出了持续免疫安全理念，结合国际领先的可信计算技术与人工智能技术，在信息系统运行的初期就通过对服务器的持续监测分析，自动生成符合操作规范的系统进程白名单和用户行为白名单，建立对关键数据的合法访问策略与操作行为策略；在威胁到来的早期对众多未知威胁进行智能分析，在监测到危害行为后，系统在人工智能技术的支持下实现对所有未知威胁的自组织对抗，并提供相应的情报以辅助决策；从而对未知威胁产生持续的免疫力，就算外部入侵者已经渗入内网，也会无所遁形毫无作为。同时，利用高速区块链技术存储审计信息，防止行为记录被篡改，最终构建持续免疫系统。

八分量推荐利用基于网络和基于主机的安全技术组合来进行深入防御的方法。八分量持续免疫系统解决方案是基于主机的入侵防御技术，可以在经济有效、集中管理的产品中提供“零日”攻击防护、操作系统和常用用户应用程序的即装即用强化功能，以及保持遵从企业管理和安全策略的能力。

客户表示他们会首选基于行为的可信计算与入侵防御解决方案，该解决方案易于使用和部署，无需病毒特征即可保护每一台计算机的操作系统功能和应用程序，从而使管理员能游刃有余地修补他们的系统。

这种基于持续免疫的方法具有以下优势：

* 能够将与病毒和蠕虫有关的停机时间和成本降至最低
* 能够将恶意行为的破坏降至最低
* 能够减少对持续应用供应商补丁程序的需求
* 能够消除对持续应用特征更新的需求
* 需要较少的持续维护
* 对 IT 资源的需求很小或根本无需额外使用
  1. 持续免疫系统的设计理念

八分量持续免疫系统解决方案基于行为定义，认为每一个软件程序以特殊方式访问某些资源以完成其任务。它必须创建或修改一些资源（例如，日志文件、消息存储、文档文件）。还有一些资源它只要读取（例如，配置数据、动态库、内容）。此外，还有大量资源它根本无需访问。许多攻击“诱使”操作系统功能（如 RPC）或应用程序修改上述后两类资源，从而造成危害。

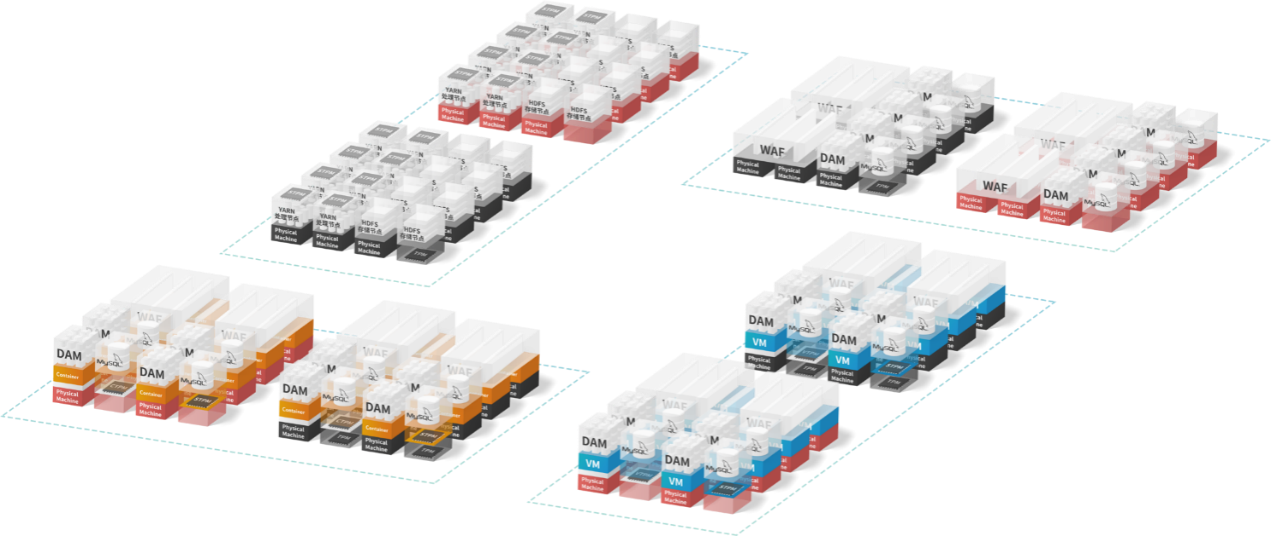
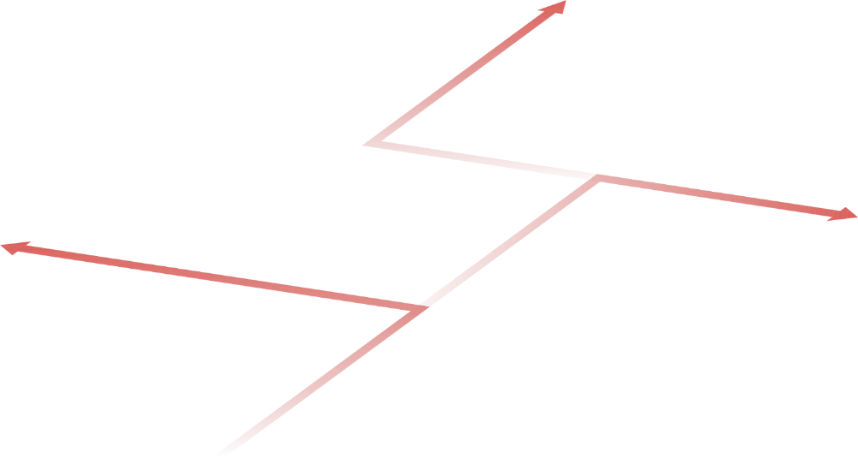
八分量持续免疫系统解决方案包含行为说明，用于定义操作系统功能或应用程序与系统资源（如文件、进程、配置文件）相关的可接受活动。无论攻击者采取何种方法访问系统，八分量持续免疫系统解决方案都能够通过实施这些行为说明，在不良行为损害系统之前先行阻止。这种基于行为的防护方法使八分量持续免疫系统解决方案能够立即抵御新攻击，而不必“弥补”基于特征的产品出现的问题或补丁程序的“零日”漏洞。

* 1. 持续免疫系统架构介绍

八分量持续免疫系统解决方案 主要由下面4大模块组成，能够部署多种复杂环境，以及对应的多种灵活的组合。部署架构包含下列主要组件：

* 可信防护：每一台受保护计算机上，秒级感知异常的加载，防御未知病毒攻击，抵御获得最高控制权的入侵者，自动生成硬件级白名单，并可以对当前进行的非法操作即刻阻断。
* 用户行为分析： 为八分量持续免疫系统解决方案提供快速识别合法用户的异常操作，人工智能用户系统日志分析，自我识别用户行为。
* 主动对抗： 用于分析网络威胁态势感知，展示客户受攻击的IP及地点，将分析的内容为主动对抗，提供重要信息，告警阻断攻击，并自动采取预判攻击之后的防御措施。
* 区块链防篡改 使用区块链系统保存行为敏感数据，提供追溯存证，防止篡改等服务以及策略，并可以对被恶意篡改的网页数据文件提供毫秒级的自动恢复。

区块链防篡改



用户行为分析

可信防护

主动对抗

图2.2-1系统解决方案

* + 1. 可信防护说明

该服务为受控保护的主机，提供可信的状态服务，由SERVER及受控AGENT组成，其中服务主要构成有：应用展示操作，数据处理，证实基础

在每一台受保护的主机上，通过特定的AGENT，通过TPM芯片获取到当前的主机状态，并加密上报，达到秒级感知状态

基础证实是以OAT处理为核心，使用白名单基础检索，达到处理证实状态，在有序的作业序列化后，通过自身CA加密传输到上层

在能力层中实现对请求的处理，白名单和验证和加载，以及其他应用层中接口的实现。

应用层中即为提供操作的入口和数据的展示，及具体使用功能，达到自动形成白名单保存，保证所保护的机器上只运行白名单中的程序，一旦有任何内外或部人员执行非白名单程序（如系统后门、病毒、勒索病毒、渗透工具），则会报警或阻断。



图2.2.1-1可信防护框架

可信防护摘要

可信防护主要以下功能：

* 探测被保护主机，自动加载
* 防控被保护主机，开启关闭状态
* 验证详细日志
* 白名单的展示和查询
* 异常确认，增加相应的白名单

关键技术

操作系统内核使用TCM技术为核心，完成主机加电后建立完整性度量。

硬件级别的白名单，会自动产生，以便秒级感知非授权程序加载。

识别非白名单列表中内的程序，认为非授权程序，做异常处理。

* + 1. 用户行为分析说明

该服务为受控保护的主机，提供智能数据分析和强策略定制，由基础数据采集，业务处理层，以及展示应用层组成。

在受保护的设备上，通过特定的技术方式，提取对应的数据，通过特定的采集层的流转，序列化成对应的大数据消息。

经过数据处理和对应的业务逻辑计算后，生成对应的事件以及数据，分别上报到应用层的不用接口和调用请求，并存储用户模型。

在应用层中实现对请求的处理，并为提供操作和画像的展示，达到人工可干预的策略定制，AI学习，报警处理等方面。

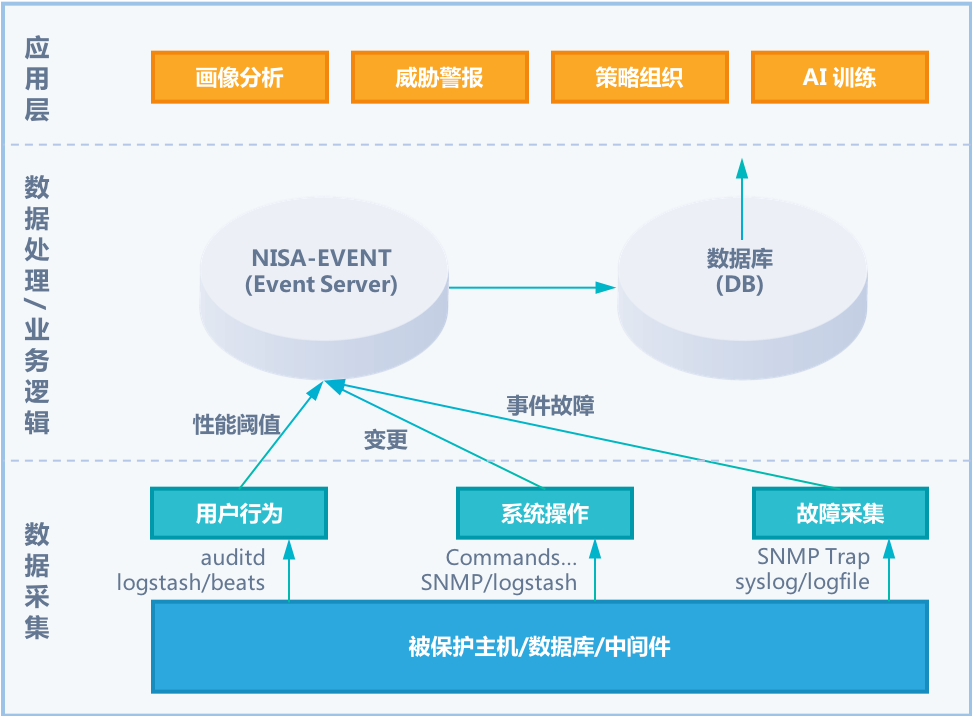


图2.2.2-1用户行为分析框架

用户行为分析摘要

主要以下功能：

* 定制人工，强制策略
* 报警的展示和处理
* 用户操作的记录和画像的展示
* AI的训练和加载

关键技术

通过AI的学习，分析生成对应的用户行为范式。

人工加载规则，设置非法操作的下限。

数据结构化处理，流转。

* + 1. 主动对抗说明

该服务为保护的整个系统，提供基础防御和检测的机制，在AI发现的支持下，针对所感知、预判的威胁，自动制定主动对抗策略。

利用容器技术，在入侵者采取下一步攻击手段之前，在扫描和初始阶段，实现第一时间响应处置。针对入侵发生的具体场景，利用大数据分析手段，智能生成威胁情报，为安全运维人员及时决策并实施人工处置提供支持。

由防控防火墙组，数据展示，基础数据采集，威胁处理，蜜网收集态势，以及审计插件组成。

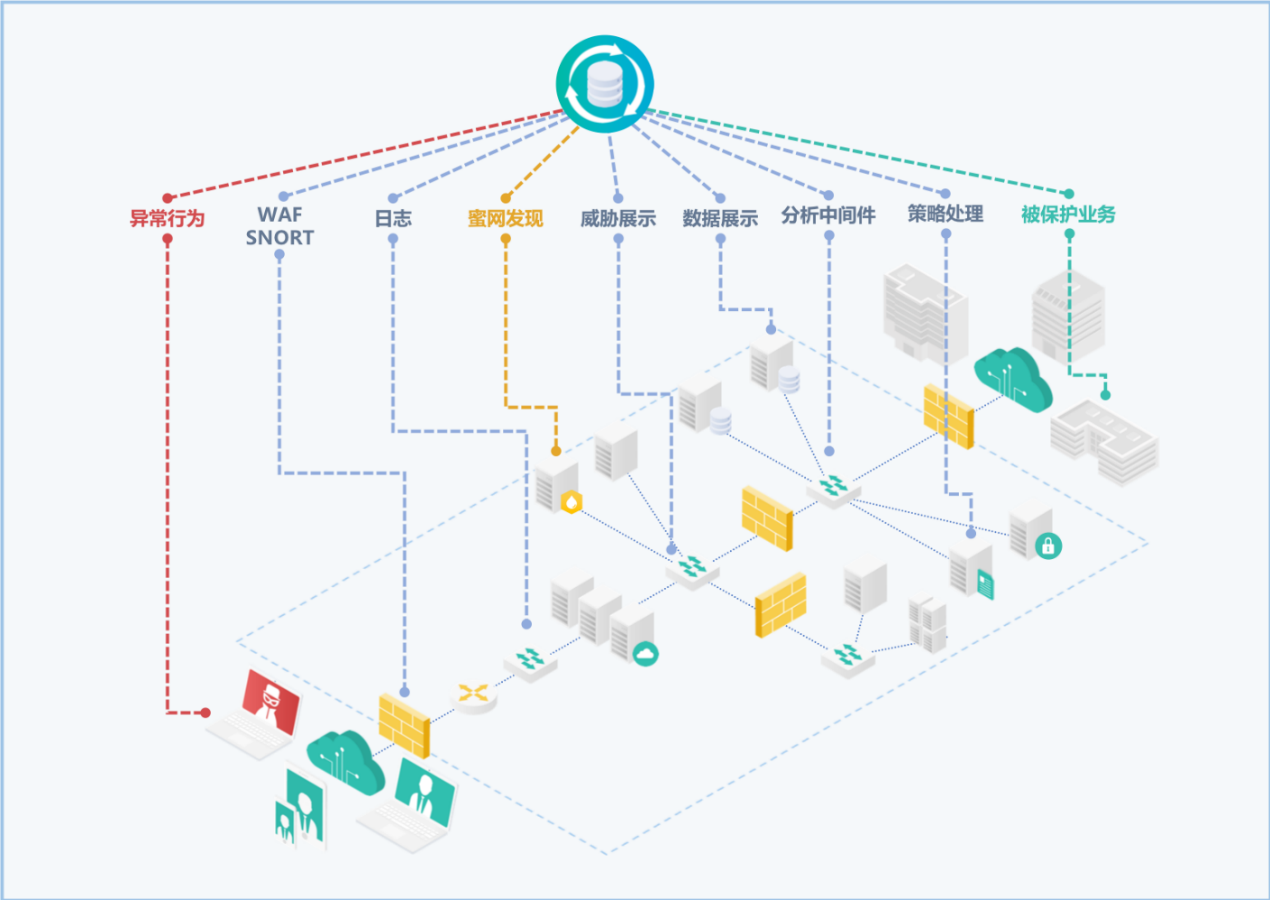


图2.2.3-1主动对抗框架

主动对抗摘要

主要以下功能：

* 信息中心，全面的被保护主机状态
* 当前的攻防态势，被攻击的进程
* 蜜网捕获的进度和状态
* 防控火墙的WAF SNORT状态
* 审计行为以及插件的应用

关键技术

蜜罐的操作系统，容器云的形式，分布到资源点中。

ELK(一个实时分布式的日志分析平台)的数据流转为依托的行为处置和格式化操作。

应用模块组件的容器化执行策略。

* + 1. 区块链防篡改说明

该服务利用八分量的区块链防篡改技术为保护系统内珍贵的数据，对一切恶意行为，进行的数据破坏，进行自动修复，保障所有审计信息、关键数据不被篡改，并保留破坏行为的记录。

同时防止内部人员，人为误操作进行的数据破坏（符合国家安全法日志需保证完整存储6个月以上）。

存储层是以区块链为核心，使用独特优化的调度方式和分布的存储空间，达到数据高效的加密存储，并防止任何潜在的方式去恶意读取。

在能力层中实现对业务请求的处理，数据的分析和序列化，以及加载审核版本等操作，还有其他应用层中接口的实现。

应用层中即为提供操作的入口和数据的展示，及具体使用功能，达到对关键数据加密保护和报警操作等。



图2.2.4-1区块链防篡改框架

区块链防篡改摘要

主要以下功能：

* 实现可信区块链的节点工作状态，以及存证数据的展示
* 合法的操作存储数据的接口
* 防篡改目录的保护以及版本状态，操作日志，用户管理等
* SVN/GIT的保护以及版本状态，操作日志，用户管理等

关键技术

特有的区块节点，来共识所存储的数据，以及提供应用的状态。

联盟链的准入和加密的行为，以及实现CA(即电子认证服务)的服务功能。

节点对外统一的7层数据实现，以及对外接口功能的实现。

1. 产品特点

**新安全新思维**

**持续免疫能力=可信+智能+人**

**机器可信：**

* 准确洞知机器的真实行为
* 主动预判机器的合法行为第一时间发现
* 定位非法行为

**智能安全：**

* 作用于安全团队采取行动之前
* 主动控制入侵者非法行为的影响范围
* 诱导入侵者犯错以争取更多响应时间

**精准防控：**

* 以精准的安全态势情报掌控全局
* 以机器学习安全响应推荐方案辅助决策

1. 产品功能
   1. 可信防护

产品通过对服务器的持续监测，可自动生成符合规范的进程白名单和用户行为白名单，并将其存入硬件芯片，赋予服务器免疫恶意程序及违规行为的能力。对于已经拿到最高权限的入侵者，系统将实时发现恶意删除、拷贝以及篡改等违规行为，并及时对这些行为进行锁定限制**。**

**1秒内感知异常进程加载**

* 当入侵者利用0Day漏洞夺取了系统控制权：
* 可信硬件级别监控，对抗ROOT权限黑客
* 万级节点环境单秒内告警，极短攻击窗口
* 细粒度白名单透明生成，最小管理复杂度



图4.1-1可信防护

**违规行为限制**

通过制定程序白名单的方式，使得即便获得了该服务器最高控制权的入侵者，也无法加载用于实施破坏的恶意程序，如系统后门、病毒、渗透工具，从而极大地限制了入侵手段。

**白名单智能管理**

持续免疫系统通过分析服务器的运维策略、运行语义自动生成服务器程序白名单，从而极大地降低了白名单的管理成本，有效降低白名单人工管理带来的潜在安全风险。

* 1. 用户行为分析

产品在分析用户行为日志和全球威胁情报的基础上，能够综合判断威胁发生的可能性、发展态势，比入侵者更快一步感知威胁。在大数据智能分析的作用下，系统可自主预判威胁程度并判断威胁级别，实时发出不同级别的告警通知，并进行归类处置。

**10秒内感知异常操作行为**

* 当入侵者盗用超级管理员密码伪装登陆：
* 大数据管理员行为分析，迅速识破盗用者异常操作行为
* 过滤 100% 异常进程，极低误报率
* 系统层操作行为分析，捕捉最细微的操作

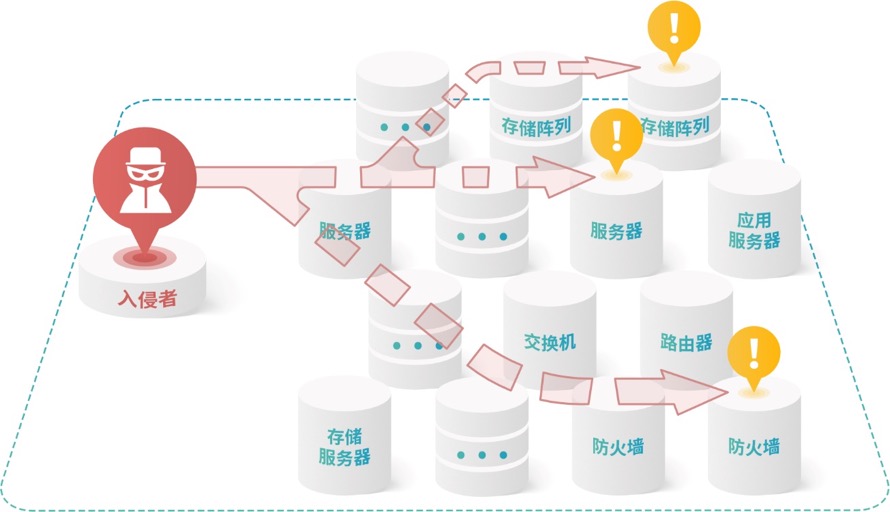


图4.2-1用户行为分析

**用户行为分析**

集合系统进程、操作日志等多数据源，聚合分析用户与系统行为，判断是否存在异常或威胁行为。评估异常事件风险程度，更聚焦的用户行为分析有助于减小误判、提高辨识速度，精准感知内外威胁。

**渗透路径预判**

鉴于攻击手段被限制、攻击行为被感知，再结合威胁情报，持续免疫引擎能够更准确地进一步匹配攻击模式、预判渗透路径、归纳威胁级别。在威胁发生之前，通过多种渠道抢先发送分级警报通知。

* 1. 主动对抗

产品在人工智能技术的支持下，能够对所有未知威胁实施自组织对抗，在发现威胁的第一时间及时响应处置，用户亦可根据业务需求进行定制化设置。产品针对入侵发生的具体场景，利用大数据分析手段，智能生成威胁情报，帮助安全运维人员及时决策并实施人工处置。

**15秒内自动部署对抗措施**

* 在告警触发到补救方案实施的时间窗口内：
* 机器学习预判入侵者攻击路径，比入侵者更懂入侵
* 人工智能主动对抗所感知的威胁，为安全管理员抢时间
* 专家系统辅助实施补救方案，比安全管理员更懂防御

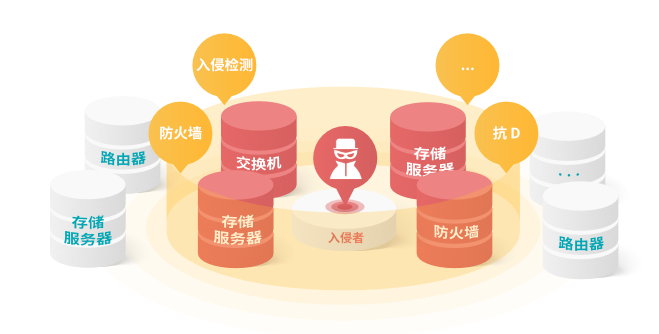


图4.3-1主动对抗

**智能自组织对抗**

在机器学习技术的支持下，针对所感知、预判的未知威胁自动制定主动对抗策略。并利用容器技术，在入侵者采取下一步攻击手段之前，在其攻击路径上高速分发安全措施，实现第一时间响应处置。

**情报辅助决策**

针对入侵发生的具体场景，综合全球威胁情报，利用大数据分析手段，智能生成针对性的威胁分析，为安全运维人员及时决策并实施人工处置提供支持。

* 1. 区块链防篡改

产品将所有审计信息均存储于高速区块链中，既能完美保护审计信息不被篡改，又能赋予信息系统抗抵赖的特性。正因产品存储所有用户行为，所以八分量能够提供高速精准的搜索引擎，方便企业对威胁其安全的信息和行为进行查询追踪。

当入侵者试图抹除系统日志以逃脱追责：

区块链系统行为存证，比特币账本级别的防篡改强度

**10万级 TPS（每秒数据存储笔数），数据库级别的存储效率**

大数据历史行为追踪，金融防欺诈级别的恶意行为追溯

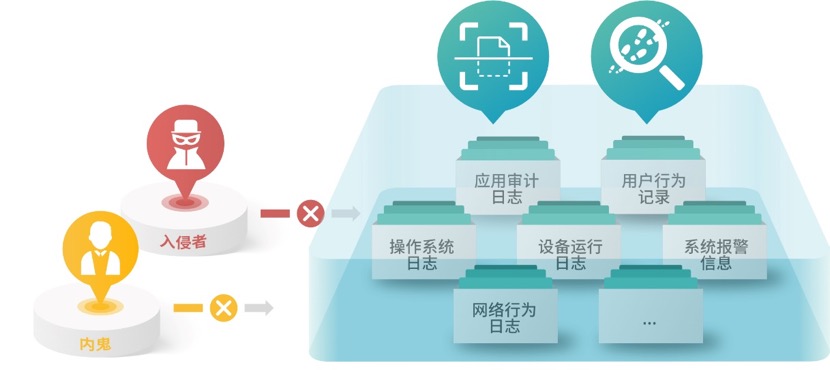


图4.4-1区块链防篡改

**数据防篡改**

利用自主研发的高速区块链技术，保障所有审计信息、关键数据不被篡改。即便获得最高控制权的入侵者，也无法抹除或修改，内部权限账户的恶意行为也不能因为其身份特殊而破坏数据的完整性。

**行为可追踪**

针对所有用户行为、安全威胁记录，持续免疫系统提供了高速精准的搜索引擎、高效智能的关联分析、多样直观的图形化展示、及丰富具体的安全报表。内外威胁风险记录均能完整追踪，提高了安全人员对全局安全态势的把控能力。

* 1. 功能介绍
     1. 首页

持续免疫系统的首页汇总了持续免疫系统的真实使用信息。方便安全管理人员通过界面直观的对持续免疫系统的所有功能进行控制和操作。其采用B/S架构，有非常方便的管理员权限控制登录系统，兼容HTTPS等安全加密通讯协议。

****

图4.5.1-1

* + 1. 可信防护

可信防护功能，满足提供给用户界面可以方便的控制被保护机器的可信防御功能的开启，关闭，白名单的管理等工作。

在该功能下，如果用户的机器处于被可信保护的状态，用户需要进行对被保护机器的操作，可以通过两种途径，一种是直接暂停当前的可信保护。然后就可以自然正常的在被保护机器上随意正常的操作，操作完再重新打开可信保护就可以重新恢复到可信状态防御。另一种是采用直接授权的运维登录（这里可以是客户自己的运维登录工具），通过可信授权后的运维登录操作，我们都会进行自动的可信计算防御分析，保证这个时候的运维操作都是属于可信状态的。除了以上两种途径，如果有用户或者攻击者使用其它途径对机器进行了操作，哪怕是管理员账号都会立刻被发现并能阻止。

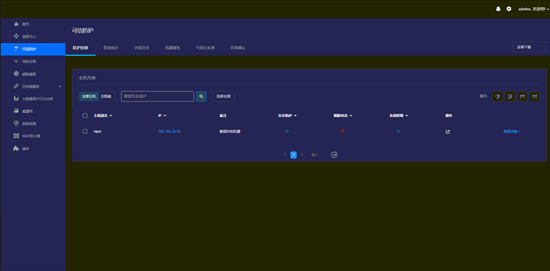


图4.5.2-1可信防御控制页面

* + 1. 用户行为分析

用户行为分析模块（UEBA）针对被持续免疫系统保护的主机的所有程序行为进行人工智能分析，主要采用深度学习+组合学习的方式。默认会对用户使用系统的一段正常时间的行为数据进行建模，一旦有使用者违反了正常行为数据的建模将立刻发现并预警。同时也支持用户通过编写人工智能系统能认知的规则，定义用户自己明确的防范条例。比如限制对于被保护系统的数据库文件，日志等的靠背的行为。

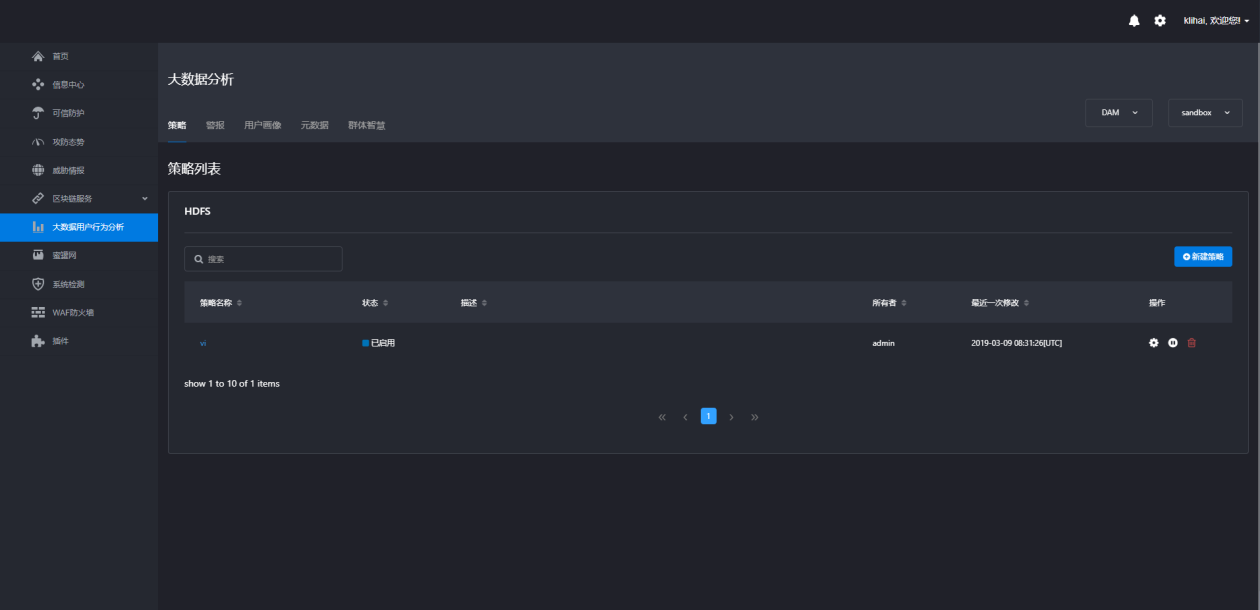


图4.5.3-1

同时持续免疫系统能对被保护机器上的所有用户进行用户行为分析，比如用户的联系方式，行为特点统计图表，以及操作历史记录。

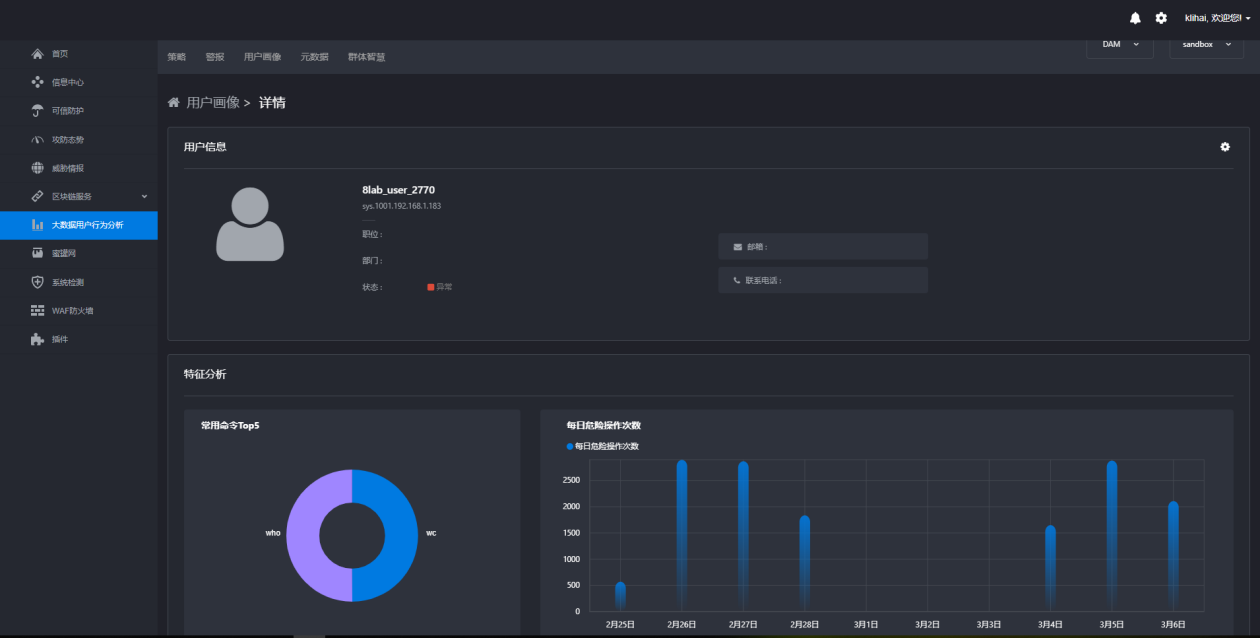


图4.5.3-2

* + 1. 全球态势感知

全球态势感知能根据当前被保护机器的感知攻击威胁，对全球的攻击信息进行聚合分析的2D/3D追溯展示，可以精确到街道。并且能根据用户的要求，方便的进行2D/3D切换。方便用户能非常直观快捷的了解到当前自己系统在持续免疫系统保护下的安全态势。3D的态势感知如下：

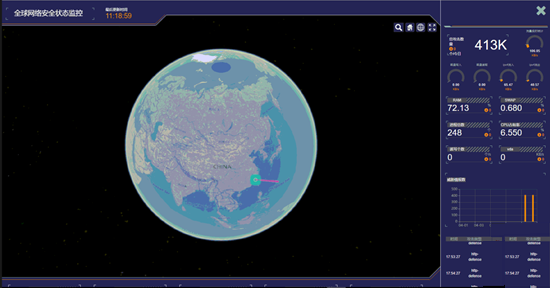


图4.5.3-1

2D模式下的态势感知如下：



图4.5.3-2

* + 1. 自适应蜜网防御功能

八分量持续免疫系统的自适应蜜网防御，是在用户的主机集群工作范围内或者边界通过容器技术搭建的蜜网陷阱，通过诱捕或者故意的缺陷，让攻击者进行访问与窃取，在攻击者访问与窃取这些陷阱的时候，八分量持续免疫系统可以立刻抓住攻击者的特征，并配合可信计算和UEBA技术来限制攻击者进一步的更大范围攻击。该功能提供了非常方便的界面控制系统，方便用户定制各种蜜网组件与陷阱事件，如下图所示：

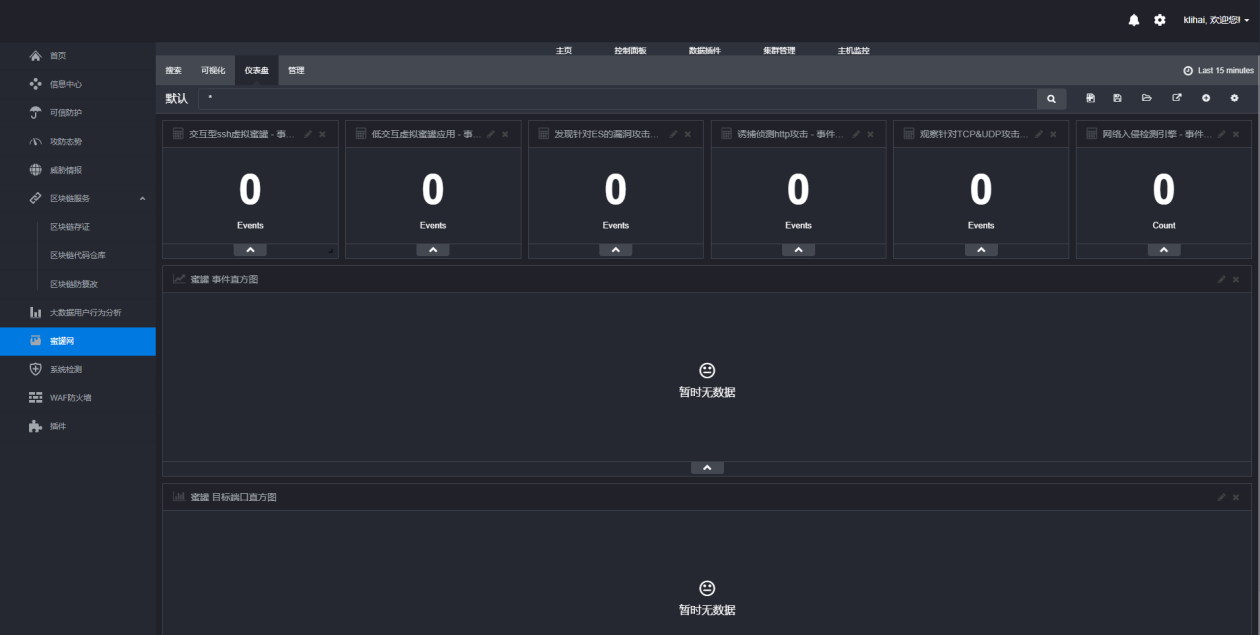


图4.5.7-1

同时也提供了直观清晰的蜜网集群的监控导航面板，方便查看各种被保护宿主机资源使用情况，如图：

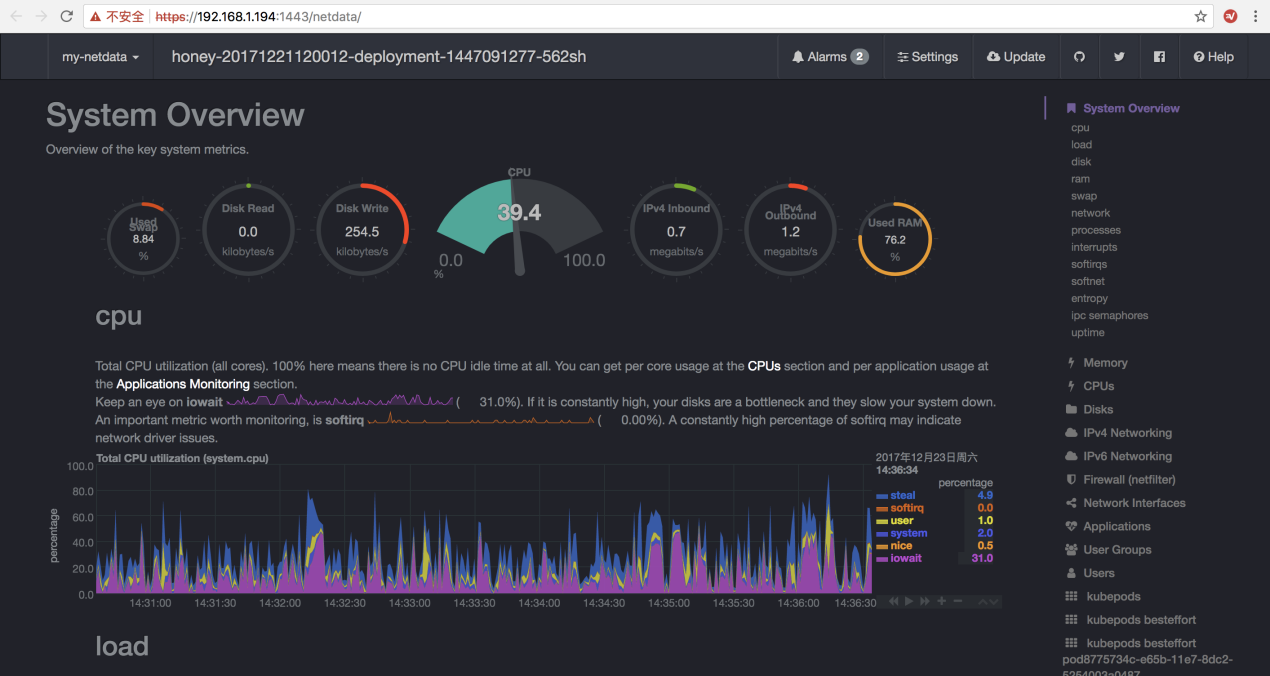


图4.5.7-2

* + 1. 区块链防篡改

基于可信区块链技术的区块链防篡改系统在使用的时候分为客户端和服务端。方便用户从管理员和用户角度分别进行关键数据在区块链上面的资产管理。

区块链防篡改服务为静态的数据目标提供持续性区块链存证的服务，最大限度的保证用户的关键数据内容安全、可控。一旦存储在可信区块链上以后，不会受到恶意的损失或者未知攻击的破坏。其在使用的时候采用的B/C（浏览器和服务器）架构，用户和服务之间通过客户端进行通讯和协作。客户端如下图：

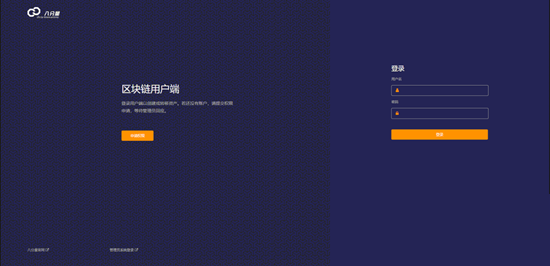


图4.5.6-1

服务端的区块链防篡改页面主要展示可信区块链的节点，拓扑整体交易情况。

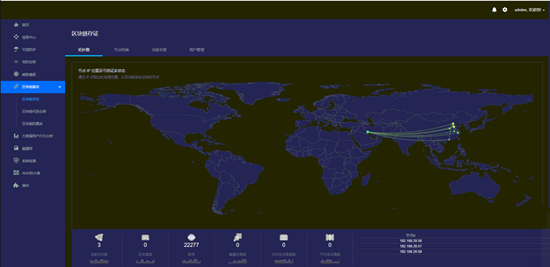


图4.5.6-2

通过区块链的展示界面可以非常方便的查看到每一笔数字交易的过程，数据拥有者，每一笔数据资产的变更转换等。

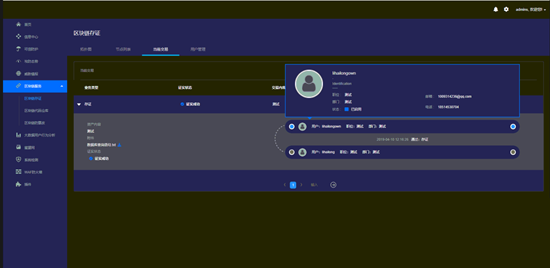


图4.5.6-3

* + 1. 日志中心

实现对所有被持续免疫系统保护的系统上面的行为日志进行统计与分析，方便用户全面的了解自己信息资产的工作情况与安全事件，能非常方便的建立对应的索引和搜索关键字，可以快速的图形化的按照时间或者索引内容，进行全文日志情况统计与展示。同时针对其展示仪表盘的形势，持续免疫系统也支持用户手动拖拽的自定义工作模式，满足用户对于仪表盘展示效果的各种要求。

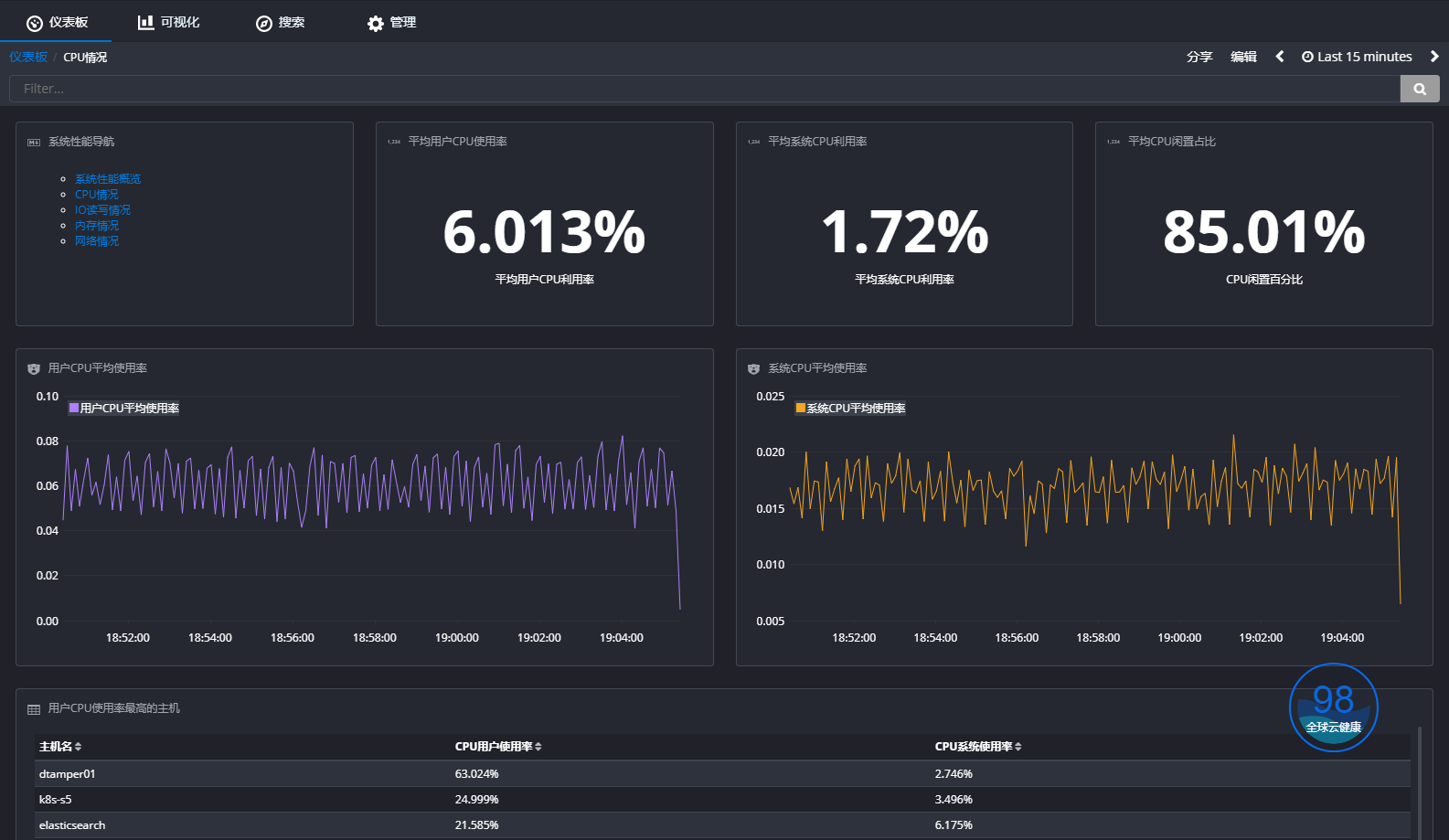


图4.5.4-1

1. 产品运维部署

八分量持续免疫系统提供多样灵活的部署方式，部分功能可以根据用户的需求支持无代理部署。

* 1. SaaS部署

针对有云服务的客户，我们可以根据其网络应用的情况，完成SaaS的部署方式，各项服务，部署在云端，通过API的形式封装 给出接口，以便客户端，来适配和请求所需的功能， 由于需要联通到API 所以主机的请求，要给出相应的访问权限，和数据传输限额，其结构如下：

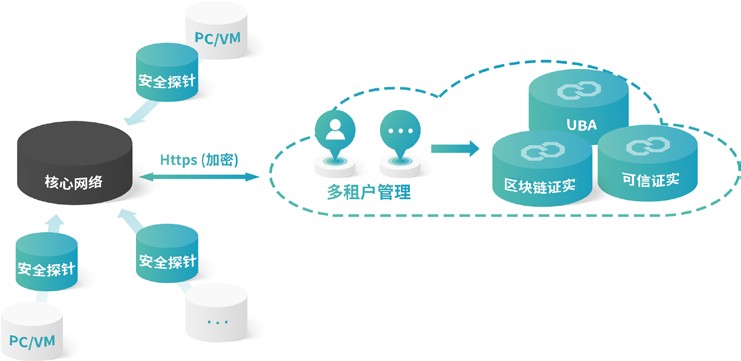


图5.1-1

* 1. 私有网物理隔离部署

对于数据管理安全比较敏感的用户，我们支持其私有部署，物理隔离的方式。私有化的服务部署，会将各个功能点，需求的主机放在接入端的内部网络，以便独立的内网主机使用，不需链接公网出口，处理逻辑都在内部完成和展示。其结构如下：

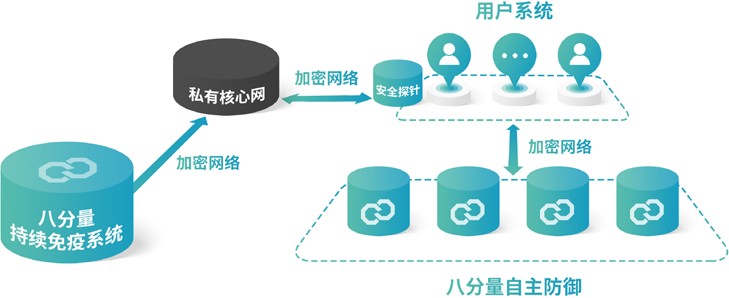


图5.2-1

* 1. 组件式布署

针对目前用户的实际应用场景，八分量持续免疫系统的4大功能模块都可以独立或者组合安装。可以根据用户的需求进行个性化的定制，也可以兼容对接用户已有的安全管控平台进行统一的调度。其架构如下：

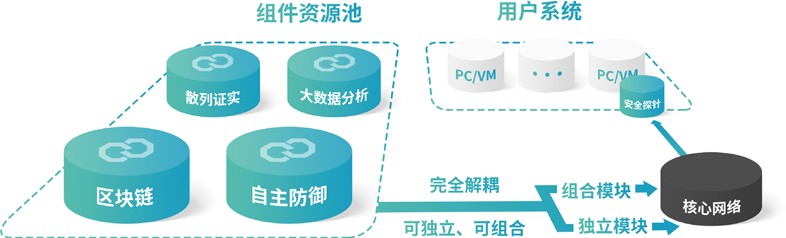


图5.3-1

* 1. 批量部署与SMDB兼容

实现批量操作系统配置、批量程序的部署、批量运行命令等功能。目前我们可以提供管理服务工作站上安装对应的程序配置被管控主机的 IP 信息，被管控的主机无客户端。或者配合由客户的SMDB系统下发，封装对应的一键安装脚本，以及一些必须依赖的组件安装。目前经过沟通，希望使用后者，通过SMDB下发到对应所需要的主机。下发过程，需要提前根据需求，定制分组的主机规则和执行的安装文件。

* 1. 持续免疫系统运维架构

八分量推荐利用基于网络和基于主机的安全技术组合来进行深入防御的方法。八分量持续免疫系统解决方案是基于主机的可信计算等入侵防御技术组合，可以在经济有效、集中管理的产品中提供“零日”攻击防护、操作系统和常用用户应用程序的即装即用强化功能，以及保持遵从企业管理和安全策略的能力。

在具体实施的时候会对客户项目需求的了解，并基于对服务器、网络设备更高可靠性的考虑，推荐具体的相关硬件设备及系统软件参考配置，后期投产需要的实际性能测试，会在POC中测试完成评估。其大型系统中应用持续免疫系统的常用推荐的运维部署架构如下图：

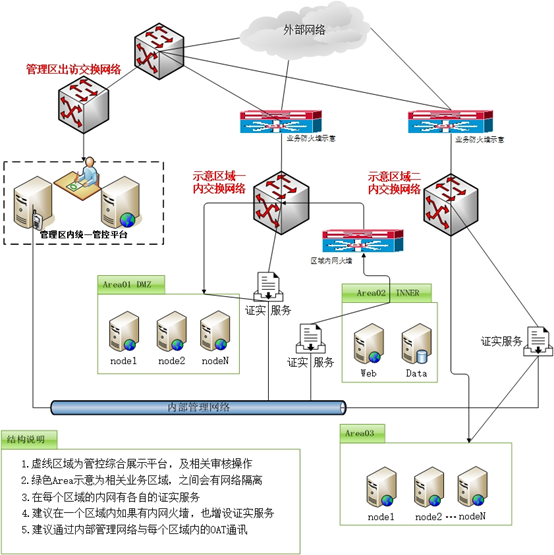


图5.5-1运维部署架构图

可以使用物理主机或虚拟主机，也可以用容器平台来启动。根据具体的需求来划分使用资源即可。

每个服务对接的被保护主机，需要根据具体的配置，要提前编制出来。

每单位服务性能，可以承载最大的度量数据，会在性能测试中体现，以供参考，实际业务中，建议根据具体的业务量级，评估度量的服务所用资源。

管理区域内统一管理平台用服务器访问web端的形式实现对管理区域内主机汇总信息的查看。

* 1. 运维分组结构

目前持续免疫系统的分组规则，是根据实际区域划分或者最大服务承载的状态来明确具体的服务分组，其具体的角色可以支持以下5种：

* VLAN（虚拟局域网）规则，基础网络规则，建议SERVER和被保护主机可以2层通讯
* 业务区域，由相关业务审查管理提供需求
* 网络区域，跨火墙区域需要有访问策略互通
* 资源满负荷运转状态下的扩容需求
* 其他需求
  1. 运维展示管控中心

运维展示管控中心主要是承载运维综合展示的平台，及配合用户系统进行相关审核操作，需要有对内部接口的开放，主要角色有：展示入口, 管理员控制台，数据存储流转服务（注意：八分量持续免疫系统本身默认已经带有相关的服务，如果用户有集成要求，可以进行定制）。

以目前八分量已有项目的POC的状态评估，在50个用户被保护的高性能服务计算资源情况下，2个可信区域。其具体配置如下表。持续面系统采用了微服务架构设计，可以方便的根据用户的业务需求变化，做弹性资源扩展。具体推荐配置如下表：



表5.7-1

* 服务器群组应建立在同一10M/100M/1000M全交换的局域子网内，需要与每个区域内的server通讯。
* 主要网络流量都在，服务主机子网内，建议100M以上子网内部交换即可，并需要与每个受控区内的server通讯。
* UEBA所需的大数据平台的交换数据，需要实时数据的审核，跨区域流量多来自于此，与每个受控区内到管控server通讯，峰值流量不会超过20M。
* 可信状态平台，需要管控到每个区域内的状态SERVER，所以也需要有访问策略，这里也会有一定的网络流量，一般都不会超过1M。同时占用的用户端CPU不超过2%，内存一般不超过54MB。
  1. 区域可信证实服务运维服务

这里主要是针对每个区域内的受控主机状态的可信审核与证实功能进行运维，以及相关行为日志的收敛，在同一个内网工作的主机，默认建议支持不超过50个高性能节点的行为控制和可信证实，其上面的日志流转按1年存储计算。

主要角色包括: 代理服务，证实服务， 日志存储。其具体配置如下：

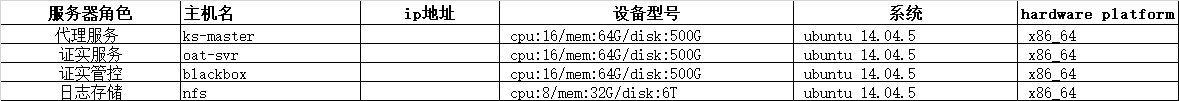


图5.8-1

* 服务器群组应建立在与被控主机同一子网内。
* 服务器需与管控的server通讯，峰值流量小于20M/S

1. 安装及配置环境与性能规格说明

持续免疫系统主要的服务资源，都建立在容器云基础之上，只要用户的环境具备有资源存在，就会保证镜像的存活。从而建立高可用的服务运行环境。

* 1. 环境要求

被保护主机推荐：Linux内核在3.8及以上

服务端和客户端其环境推荐：Ubuntu 14.04 CentOS 7.0及以上的64位系统

如果需要持续免疫系统能自动化部署的主机上，请在部署安装的时候提供临时的root 账户和密码访问其他主机的权限

注意：以下具体环境的ip 请参考对应主机表进行修改，本文中，用x.x.x.x 代表需要修改的ip 部分

* 1. 安装主机脚本分布概况举例

|  |  |
| --- | --- |
| 源主机 | /data/soft.tar.gz  /data/pypi.tar.gz  /data/local-source-list.sh(若自动化主机和源主机为同一个，则在原来的目录中即可) |
| 自动化部署主机： | /data/*项目目录*; |
| 数据库主机： | deploy-database.sh  sql目录 |
| es 主机： | /root/deploy-format.sh  /root/deldata.sh  /root/jsonfile.tar.gz  /root/esdump-node.tar.gz |
| Resistry主机： | /data/images/\*.tar (镜像们)  deploy-imageshub.sh |
| k8s-master：（一般为k8s-s1） | /data/yaml-files |

表6.2-1

其对应的服务端的配置和性能在5.7和5.8节已经提到，这里再强调一下。

* 1. 服务端配置和性能指标

保护50个高性能计算资源的推荐配置如下表：



表6.3-1

关键性能指标说明：

* 服务器群组应建立在同一10M/100M/1000M全交换的局域子网内，需要与每个区域内的server通讯。
* 主要网络流量都在，服务主机子网内，建议100M以上子网内部交换即可，并需要与每个受控区内的server通讯。
* UEBA所需的大数据平台的交换数据，需要实时数据的审核，跨区域流量多来自于此，与每个受控区内到管控server通讯，峰值流量不会超过20M。
* 可信状态平台，需要管控到每个区域内的状态SERVER，所以也需要有访问策略，这里也会有一定的网络流量，一般都不会超过1M。同时占用的用户端CPU平均不超过2%，内存平均不超过54MB。
  1. 可信证实配置和性能指标

默认建议支持不超过50个高性能节点的行为控制和可信证实，其上面的日志流转按1年存储计算。主要角色包括: 代理服务，证实服务， 日志存储。其具体配置如下：

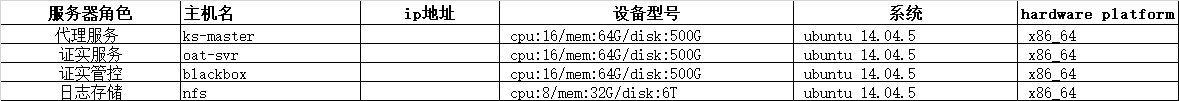


表6.4-1

* 服务器群组应建立在与被控主机同一子网内，通讯延时不超过3秒。
* 服务器需与管控的server通讯，峰值流量小于20M/S。
* 内存占用率平均不超过30MB，CPU平均不超过3%。

1. 产品优势

|  |  |
| --- | --- |
| **传统安全防护** | **八分量持续免疫系统** |
| **永不停歇的“漏洞- 补丁”循环**  无法自动验证运维结果的正确性。  通过定时漏洞扫描、安全事件分析，查询系统脆弱性。  对威胁的感知受限于威胁黑名单的丰富程度。发现威胁时往往损害已经产生。 | **合法运维即自动免疫**  主动判断运维结果是否真实反映管理员意图。  自动创建系统的进程白名单，以锁定运维后状态。  自动抵御木马病毒、渗透工具等恶意程序的加载， 构建系统对未知威胁的免疫力。 |
| **防护机制被“ROOT”绕过**  软件实现的监控探针，当系统被攻破时易被绕过。  监控事件数据量大，监控、验证间隔以数十秒甚至数分钟计，反应不灵敏。  中心化的监控服务，可靠性低、安全性弱、抵御内部入侵能力不足。 | **可信硬件秒级监控**  基于可信硬件的监控探针，唯有物理攻击才能破坏监控机制。  利用哈希链技术呈现监控事件，比较一个整数即可验证系统状态正确性，实现了微秒级验证间隔。  去中心化的监控服务架构，有效抵御针对监控服务自身的攻击。 |
| **传统老旧的数据访问控制**  数据访问控制功能由应用软件系统自行实施。数据密钥由软件系统存储、管理，获得最高权限的入侵者盗取密钥后患无穷。  加解密数据均需要通过修改数据处理程序实现。 | **用软件行为属性解锁数据**  使用可信硬件存储数据访问密钥，抵御获得最高权限的入侵者盗取密钥。  利用数据处理程序的行为作为密钥的访问依据，主动抵御恶意程序访问加密数据。  透明加解密，数据处理程序无需修改即可访问加密数据。 |
| **运维、审计数据被篡改**  恶意运维人员篡改运维策略或脚本，导致恶意程序或非法配置信息被认为是合法操作。  获得最高权限的入侵者、“内鬼”在完成攻击行为后删除审计信息，阻断威胁追踪、损失追责路径。 | **区块链级可信审计**  所有运维策略或脚本均被区块链审计，并及时报警违规操作，让恶意行为无法隐匿。  基于区块链技术，审计数据的篡改、删除难度极大。 |
| **单一维度威胁感知**  对系统过往行为建模分析异常，难以察觉新型攻击模式，易出现误报、漏报。 | **攻击者思维的态势感知**  从系统行为趋势、入侵者可能的攻击方式综合分析安全态势，以攻击者思维考虑安全态势，“想”在真正入侵者之前。 |
| **面对新型未知威胁束手无策**  基于管理员预先配置的策略决策威胁应对措施，对管理人员的技能储备要求极高，难以应对不断变化的攻击手法。  安全措施的响应速度以数十分钟计，贻误威胁对抗的最佳时机，带来较大的损失窗口。 | **瞬时主动对抗威胁**  基于安全态势，智能预判安全措施，自动化对抗未来威胁。  提前配置、秒级部署安全措施，将威胁扼杀在萌芽之中。 |