ThreatBook
微步在线

OneEDR 产品技术白皮书

微步在线-主机威胁检测与响应平台
（OneEDR）V1.1 产品技术白皮书

2021 / 2/25

微步在线科技有限公司
LEADER IN THREAT DETECTION AND RESPONSE

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改或撤回，恕不另行通知。

北京微步在线科技有限公司已尽最大努力确保本文档内容准确可靠，但不提供任何形式的担保，任何情况下，北京微步在线有限公司均不对（包括但不限于）最终用户或任何第三方因使用本文档而造成的直接或间接的损失或损害负责。

建议该文档所含的技术操作由专业人员进行。

联系我们

如果您需要联系我们，请发送电子邮件或致电：

邮件：contactus@threatbook.cn

电话：010-57017961

或访问 https://threatbook.cn 获取最新联络信息。

目 录

一、前言

近来，网络规模不断扩大，业务服务部署模式日益复杂，传统 IDC 机房、私有云、公有云通常在一个企业中以混合结构出现。且云架构带来的多层的工作负载环境产生了数以万计的服务器，伴随而来的问题便是保障服务器主机安全的难度增大。服务器主机作为企业的核心资产，没有服务器主机安全就没有业务安全。无论是云主机还是传统 IDC 中的实体服务器，其安全保障受到越来越多的关注，已经成为企业安全的“最后一道防线”。服务器失守带来的安全失控，不仅影响潜在的系统稳定性，导致业务运行可能出现问题，更有可能带来信息泄露，进一步导致经济和品牌价值的损失。对主机入侵的实时检测和快速响应，是目前企业安全建设的重要方向，在传统杀毒之外，更加有效的针对服务器设计的检测响应平台（EDR，Endpoint Detection and Response）是当前安全环境下的大势所趋。

虽然市场上已有多款主机安全产品，但大量政企客户反馈，大多数产品在全面入侵检测方面并未达到满意水平。目前市场上有偏资产识别类的主机安全产品，侧重点在资产清单和漏洞扫描；有偏云主机管理类的主机安全产品，侧重点在公有云主机资产管理和常见木马的检测；有偏防护类的主机安全产品，侧重点在主机恶意软件查杀上。而在针对服务器的入侵检测方面，当前产品都存在较大的短板和不足。

因为当前黑客入侵主机方法复杂多样，新型的攻击手法、工具层出不穷，而传统产品集中在漏洞发现、资产清点和病毒查杀上，难以在入侵的第一时间检测到威胁。以最常见的 Webshell 为例，传统杀毒无法查杀，漏洞发现对此无效，攻击者利用多种绕过方式让网络上的安全防御失效，很多企业通过手工排查后甚至发现 Webshell 已经在被上传了数天甚至数月。即使是通过手工方式发现了也存在着溯源难、清理难的问题。

结合以上现状和难题，微步在线发布了 OneEDR，该是一款专注于入侵发现、自动化分析溯源的主机安全产品。得益于微步在线多年来在网络威胁情报，网络入侵检测能力，以及海量木马和恶意脚本分析上的积累，OneEDR 具有全面的入侵检测能力，同时凭借其业界领先的威胁情报，可以做到误报率低于 0.1%，运维人员可以集中精力，聚焦真实威胁。并将发现的威胁告警自动化聚合为事件视角，帮助用户理清一个完整的入侵事件，掌握攻击者的攻击路径，高效溯源指导快速地响应。

二、产品功能和优势特点

OneEDR 是一款关注于主机入侵检测的新型检测与响应平台，基于轻量级的终端采集和分析 Agent，通过收集终端的网络、进程、文件等行为事件，在平台侧利用威胁情报，文件检测与行为分析等技术手段，实现对主机入侵行为的精准发现、攻击路径自动化回溯，并支持对终端海量行为进行检索，同时支持对恶意入侵行为进行响应阻断。

2.1 产品功能

2.1.1 全面且精准的主机入侵检测

2.1.1.1 集成业内领先的威胁情报

在态势感知、威胁检测的建设大潮中，威胁情报成为必不可少的技术支撑，威胁情报有助于提高安全检测产品的检测效率，并降低产品的漏报率和误报率。以威胁情报订阅为基础的入侵检测设备已成为企业标配。OneEDR 集成了行业领先的微步在线威胁情报检测引擎，让全球最新的威胁情报数据和微步在线专业的威胁分析能力触手可及。微步在线的威胁情报具有高覆盖度，高精确性的特点，全面覆盖全网 99%的已知威胁，准确度达到 99.9%。针对已检出的威胁事件，情报引擎会提供其近期网络安全流行趋势和有针对性的行业趋势分析、关联的历史攻击样本信息等。

OneEDR 内置的威胁情报检测引擎会自动从云端拉取最新的威胁情报数据到本地，并结合主机的网络活动、进程活动等进行判定，检测发现主机被控的网络外联行为，以及恶意进程和恶意文件。同时基于威胁情报提供的上下文信息，可准确获得对应的威胁类型、威胁描述、关联的攻击者、关联的攻击事件、严重级别等，帮助更准确的判断并评估安全风险。

2.1.1.2 漏洞利用检测

黑客入侵主机最常用的方法之一是漏洞利用，通过查点、扫描等方式获取系统漏洞，并利用漏洞进行入侵。准确检测到利用漏洞入侵，是主机安全检测产品的必备能力。目前市场上的主机安全产品，更多基于资产信息进行漏洞发现，而不是关注漏洞利用行为的检

测能力。为了实现全面的漏洞利用检测，OneEDR 团队除了第一时间跟进最新的漏洞，提炼利用特征保证检测的覆盖度，并提供精确的修复建议。同时，通过对大量漏洞利用入侵事件的学习总结精准提炼漏洞利用的通用行为模式，并将其应用在 OneEDR 的检测引擎，实现对于未知漏洞利用行为的检测。

2.1.1.3 全面木马检测

当前木马种类多样且隐蔽性越来越高，传统杀软基于签名的检测与查杀方法，滞后于新型变种和新型攻击方法，已经不能满足当前主机端木马检测需要。OneEDR 在平台侧和 Agent 侧均内置多款自研木马检测引擎，全方位精确检测木马威胁，包括威胁情报检测引擎，基于规则的木马行为检测引擎，基于机器学习的算法模型检测。

微步在线安全云每日可采集百万级别的新增恶意样本，样本会在云端智能沙箱运行获取运行行为，OneEDR 团队会利用这部分云端行为数据，提取木马的特定行为特征，或自动训练模型，将这些特征和模型应用在平台侧和 Agent 侧，可以有效检测已知和未知木马。支持检测的威胁包括 Rootkit 木马、挖矿木马、勒索木马、僵尸网络、WebShell 等。

2.1.1.4 覆盖攻击链各阶段的行为检测

黑客的入侵方法层出不穷，攻击环节也越来越多，仅仅靠单点防御无法防护所有攻击。依托 ATT&CK 框架，OneEDR 对攻击链上的各个阶段进行威胁检测，不放过任何有可能出现在攻击链上的威胁，包括在初始入侵阶段的异常登录和爆破、作为常用入侵执行手段的反弹 Shell、成功入侵后的主机提权威胁和内网横移威胁、以及后续隐去踪迹的躲避检测威胁等。OneEDR 检测能力覆盖攻击链路的几十个攻击点，让黑客的全链路攻击无所遁形。

2.1.2 自动化事件聚合

企业安全系统的产生数十万、百万的告警，存在大量的误报，同时对外开放的业务系统每天也会面对的互联网上大量的自动化扫描和攻击，安全运营人员面对如此海量的报警，无法判定哪些是真实的攻击，哪些是针对性的攻击，哪些是成功的攻击，面对重大入侵事件，溯源与分析也无从下手，极大降低了安全检测与响应的效率。

OneEDR 提供的智能聚合功能，通过化繁为简的方式将十万、百万计的报警，自动关联聚合成可处理的数条事件，对海量攻击报警进行自动归并。该功能可自动化追溯攻击者的攻击全链路，从哪个点侵入成功，应用何种攻击手法和工具，是否存在网络外联，是否进行主机提权，是否破坏系统或者攻击内部其他机器，是否存在数据窃取。传统的检测设备对可疑日志进行告警，发现的是攻击点。而 OneEDR 对相关联的告警日志进行智能关联，以事件维度进行告警，告警的是攻击线和面。既要看到攻击结果，还要看到攻击的过程，更要看到攻击前后的完整上下文。从而更加了解攻击者的心态、意图、手法、攻击流程，影响范围。OneEDR 对攻击链路上不同阶段的告警进行智能聚合，以“威胁事件”为维度显示整体攻击的上下文。并根据攻击手法和攻击技战术对攻击者进行识别和归类，将同一团伙的攻击者放入一个事件。节省了企业运维的人力，让安全运营人员集中处理一个个事件，而不是手动关联溯源海量告警，大大提高了运维效率。

OneEDR 为每个威胁事件提供相应的威胁信息，辅助安全运维人员理解事件详情和更好地处理事件。比如每个威胁事件都会有该事件的“严重等级”，展示威胁事件的整体严重情况；每个威胁事件都会有该事件的“威胁阶段”，展示该事件目前所处的攻击链阶段，系统地了解该事件处于黑客攻击的哪个环节，帮助安全运营人员从宏观攻防角度理解事件；也支持对每个威胁事件添加处理状态并备注处理信息，同时支持多人对同一事件进行标注。

2.1.3 多视角与可视化跟踪主机入侵过程

OneEDR 针对安全运营中对于威胁监控、安全事件分析与定级，威胁溯源与处置提供了不同的视角，提高了安全团队的工作效率，保障业务系统和数据的安全性。

其中针对威胁监控，提供全面的监控 Dashboard，为目前服务器的整体安全态势进行评级，对威胁监控通常关注的主机、安全事件等提炼关联知晓，并展示最新和高危的威胁主机和事件。可帮助威胁监控人员能一览整体安全现状和重要事件。以决定是否要进行深入分析。

针对安全事件分析与定级，提供了针对特定安全事件和主机的分析页面，提供安全事件的详细的上下文，攻击对手信息、攻击手法、入侵工具、是否提权等，帮助安全运营人员快速分析并为安全事件定级。

针对威胁溯源与处置，提供了自动化溯源能力，可以将不同的威胁告警按照攻击特征的同源性自动归类为告警事件，再借助“事件回溯图”的可视化能力，自动化地将相关的

机器、攻击对手、攻击工具、攻击资产等进行关联，同时对单一告警提供“进程链图”的可视化能力，自动化定位到告警源头。并支持对告警机器的所有行为进行检索分析，辅助定位与分析，帮助安全团队快速分析攻击路径、定位恶意进程、自动检索得到关联的其他异常行为。

2.1.4 日志调查自定义检索，详细记录主机活动

无论是检测平台触发的告警，还是通过外部其他手段发现的服务器可能存在的风险情况，通常需要安全分析人员上对应的主机进行数据采集并分析，采集方式复杂且不统一，对人员要求很高。同时当发生重要威胁时，还需要进一步定位其他机器或者关联其他机器行为时候，需要扩大主机分析的范围。这对安全运营者来说难度是非常大的。而 OneEDR 通过轻量的终端采集工具，采集终端上的进程、网络、文件等关联的行为数据，并为这部分数据提供丰富的检索能力。

OneEDR 提供 SQL 语法查询，可让分析人员快速入手，同时提供筛选的字段超过 80 个，并支持多条件组合筛选，用户可自主选择如威胁主机上的所有行为，同类型账号的关联行为、关联同一个恶意工具或恶意访问地址的所有主机等。OneEDR 为企业提供 TB 级别的数据快速检索能力，单一设备可支持保存 1000 台机器 30 天内的所有行为的存储和秒级的检索能力。

2.1.5 一键处置威胁快速响应

2.1.5.1 快速响应

安全威胁事件一旦出现，相关的企业需要具备快速分析和响应的能力。仅仅检测出威胁但是没有强有力的响应手段也是没有完全解决安全威胁问题。OneEDR 集防御、检测、响应于一体，提供足够的响应能力。部署后，在 web 端操作即可对 Agent 所在服务器进行关闭进程，隔离文件，封 IP，主机断网等响应操作，可在数秒内响应安全事件并且将响应结果可视化地呈现给用户，完成安全威胁问题处理的闭环。

2.1.5.2 收集用户反馈，自适应更新检测算法

企业业务安全场景复杂，如果检测规则和算法不适应企业业务场景将会产生大量误报，增加安全运维人员的工作量。OneEDR 提供告警处置与反馈功能，安全运营人员可以跟进溯源结果处置告警，并将告警标注为真实攻击、有效告警、或者误报，并可提供文本注释，方便事后查询。OneEDR 检测引擎会收集反馈结果信息，利用机器学习算法持续优化检测算法，打造专属该企业的检测引擎系统，有针对性的加强企业检测能力。

2.2 优势特点

2.2.1 检测能力全面

当前黑客入侵方法复杂多样，入侵检测的覆盖面广度远远没有达到保证业务安全的要求。OneEDR 中集成了业界前列的微步在线威胁情报，微步在线威胁情报以专业度最高且覆盖面最广业界闻名，能全面检测入侵威胁，绝大部分常规入侵都能被发现。

当前木马工具复杂多样，检测难度高且覆盖环节较广。OneEDR 在漏洞和木马检测规则是使用通用技术总结检测，已知和未知的恶意木马都可检测到。同时采用多点布控、全链路检测的策略，完整覆盖整个攻击链的环节，真正做到让木马无所遁形。

在异常检测方面，OneEDR 采用 AI 机器学习技术对主机行为进行分析预测，及时发现主机异常行为。全面侦察到关于主机安全的行为，一举一动都尽在掌握，一旦发现异常便迅速报警，真正做到“将安全威胁扼杀在摇篮中”。

基于微步在线专业威胁情报、启发式的漏洞、木马行为特征检测、文件静态和动态监测、基于 AI 的终端行为数据异常分析模型等机制，微步在线 OneEDR 提供了全面覆盖勒索病毒、Shell、后门类木马、主机提权、僵尸网络、挖矿威胁、虚假内核、远控工具、恶意环境变量、漏洞利用、恶意进程、账号爆破等多种几十种威胁类型，全面检测已知和未知的攻击和威胁。

2.2.2 检测精度高

当前主机每天面对的攻击成十万、百万计，但有效告警屈指可数，大量告警只是攻击方在网络上的随机扫描和探测，或者是由于检测规则不准导致了大量的误报，这些都是主机安全防护中的“噪音”。太多告警“噪音”导致企业有限的安全运营人员无法聚焦在真实有效的攻击上。

OneEDR 能够精准发现入侵，准确率高达 98%。一方面，OneEDR 接入准确率达 99.99%的情报，这些情报会用于直接的威胁检测，或者用来和其他的算法、模型进行配合以提升检测的准确度；另一方面，OneEDR 将所有单点检测告警进行关联，生成攻击事件，并对一次攻击事件进行全链路取证，明确黑客攻击链路方才告警，做到极少误报。此外，OneEDR 不断收集用户的处置反馈，学习误报告警特征，不断优化机器学习算法，使其具备针对单一用户环境的适应性，进一步降低误报。

2.2.3 自动追溯攻击链，可视化展示攻击事件

OneEDR 智能挖掘告警之间的关联关系，对多条告警进行自动聚合，以“威胁事件”为维度显示整体攻击的上下文，对同一团伙的告警进行是识别和分类，帮助安全运维人员在大量告警中更高效地理清安全事件的脉络，更有针对性地去处理安全事件。

同时在处理安全事件的过程中，OneEDR 提供“事件图”和“进程链图”，实现对安全事件的可视化，理清安全事件的来龙去脉，直观展示安全事件涉及的用户，主机，进程，IP 等实体的关联关系。同时将每个告警和事件按照 ATT&CK 模型进行映射，帮助分析人员快速掌握当前攻击状态与手法。

2.2.4 轻量级的主机 Agent 对现有业务零影响，并提供全面采集能力

OneEDR 的 Agent 采用轻量化设计方法，支持多 Linux 发行版本，实现用户态数据采集，不对内核层做成影响。Agent CPU 消耗控制在 2%以下，内存消耗控制在 100MB，对系统影响极小。同时在终端上应用数据过滤和压缩技术，可控制采集数据量平均在每天 20M 左右，对网络带宽影响小。

Agent 提供了丰富的数据采集能力，可采集主机上的网络访问、文件操作、进程执行、用户登录、计划任务等多种行为，并提供各类行为数据的详细上下文，比如进程执行可详细记录等。

2.2.5 联动 TDP 赋能企业纵深防御体系，实现端+网的全链路溯源与响应

OneEDR 支持与微步在线产品 TDP 的产品联动，结合 TDP 流量数据定位入侵点，OneEDR 溯源攻击过程并且一键快速处置威胁。极大增强企业对 Webshell 木马的检测溯源能力，同时针对失陷外连主机更好地定位与溯源，从网络层和主机层双维度加强企业安全纵深防御能力，实现端+网的全链路溯源与响应，完成攻防演练环节中的处置与溯源。

三、系统架构

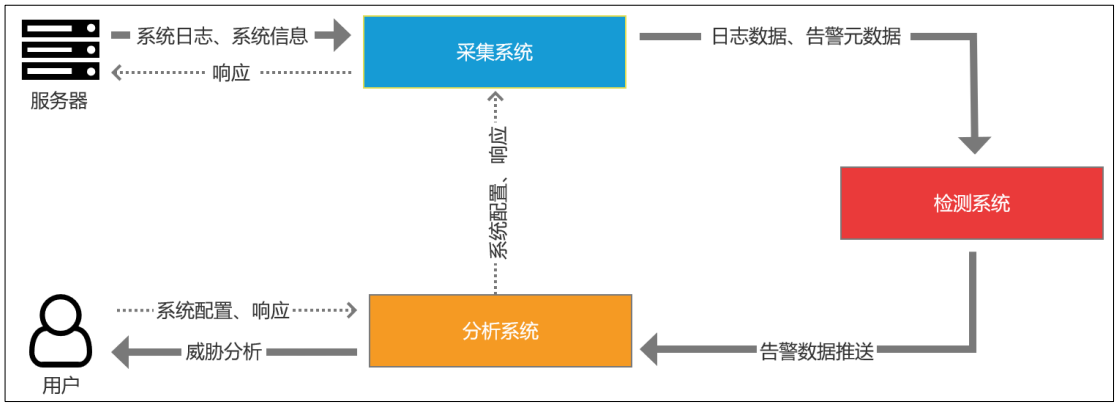
OneEDR 从整体架构上由三部分组成，分别是采集系统、检测系统和分析系统。每个系统具体负责的功能如下：

采集系统：主要负责主机日志信息和系统信息的采集、过滤和聚合，并上传相关数据到检测系统，同时支持接受相关配置的功能、支持端上木马检测功能。主要功能有数据采集、数据清理、终端检测、数据上传、应急响应、自动升级、性能监控等。

检测系统：OneEDR 检测系统是基于大数据分析的实时入侵检测平台，集成了微步在线情报引擎，行为检测引擎和恶意文件检测引擎，同时支持微步在线云沙箱检测，全面且实时地检测入侵事件的完整攻击链路。

分析系统：主要负责威胁事件的聚合、可视化展示分析以及日志调查溯源，提供面向企业安全运维人员的分析视角，提高分析溯源效率。同时提供配置接受服务，用户可在 Web 页面进行相关配置，将配置命令下发到服务器端。

三个系统之间的运转关系如下：

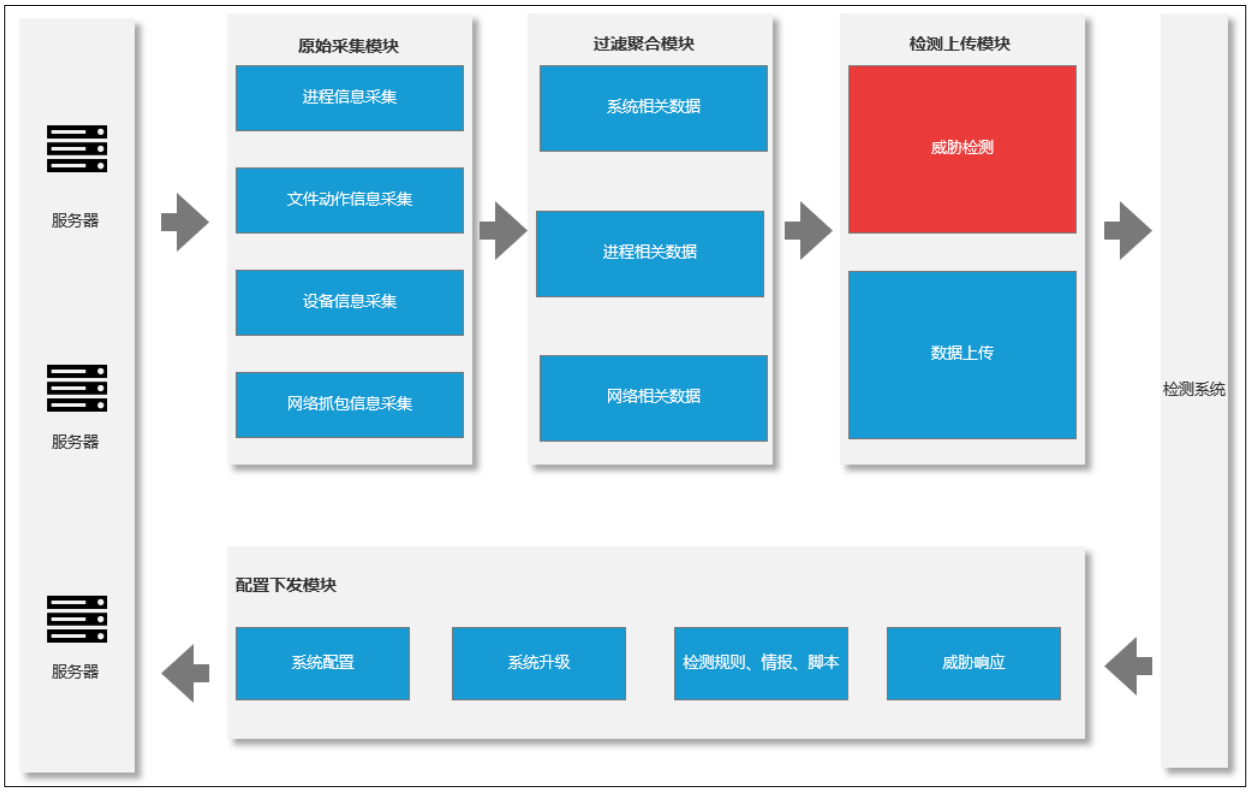


采集系统收集服务器的系统日志、系统信息，进行处理过滤后上传到检测系统；检测系统进行对相关数据信息进行分析处理形成告警数据并将分析结果保存到数据库供前端调用；分析子系统将告警数据进行聚合提炼，用户可对威胁进行可视化分析、日志数据溯源和导出，提升安全运营效率。

同时，配置命令下发、数据包的升级与反馈由分析系统直接传递给采集系统，保证系统对终端模块的控制，在主机发生威胁时做出及时响应。

3.1 采集系统

采集系统由原始采集模块、过滤聚合模块、检测上传模块和配置下发模块组成。



其中包括的主要功能有数据采集、数据清理、终端检测、数据上传、应急响应、自动升级、性能监控等。

数据采集：数据采集功能的主要作用是采集主机上的原始信息，包括主机进程信息、文件动作信息、设备信息、网络相关信息等，系统详细地了解主机设备情况以及网络安全状况。

数据清理：原始采集模块采集的信息数据会推送到过滤集合模块，在该模块中，会将大量原始采集的数据进行过滤聚合，先跟进用户自定义的白名单过滤对当前安全情况判断不重要的信息，然后将过滤完的信息进行聚合，提高检测分析的效率。主要将数据聚合为系统相关数据、进程相关数据和网络相关数据。

终端检测：采集系统的检测上传模块中提供木马威胁检测功能。终端软件 Agent 安装在主机中，提供木马后门检测，木马行为检测等基础威胁检测能力，是作为系统威胁检测的第一关。

数据上传：检测上传模块将采集并过滤聚合后的全量日志和检测后产生告警的数据上传到检测系统，保证数据传输过程中的完整性和可靠性，在传输过程中不会影响主机系统正常业务运转。

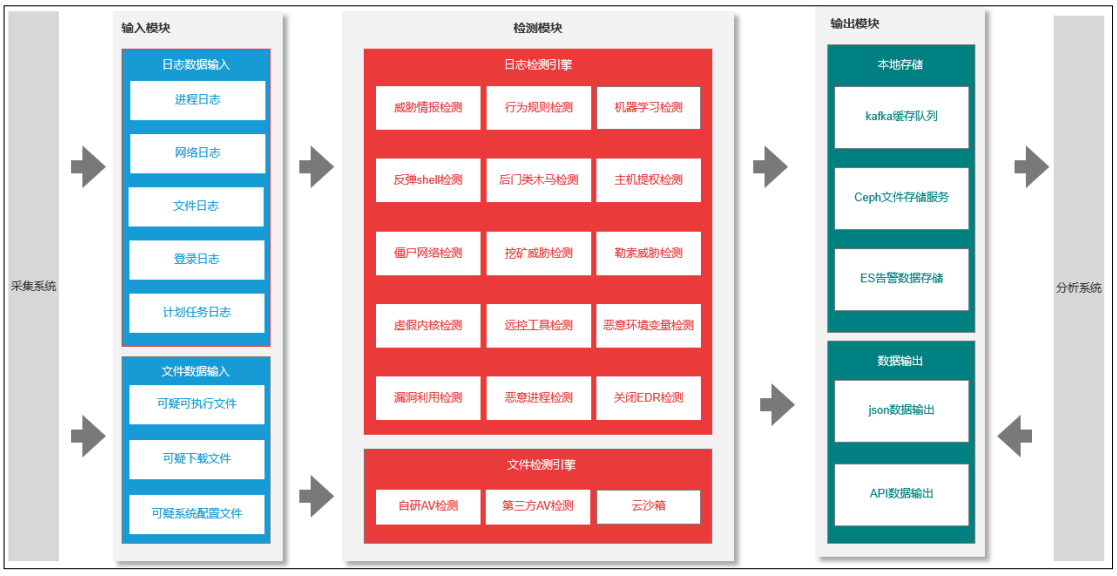
应急响应：当检测到服务器产生相应威胁时，配置下发模块可以接受来自服务端的响应命令，对主机内的威胁做到即时处置响应，包括隔离主机、隔离用户名、隔离文件、杀死进程等应急响应操作，第一时间保护主机安全。

自动升级模块：配置下发模块负责将相关配置、控制命令、系统升级安装包等下发到终端主机，实现系统对终端的协同控制。同时也会下发最新检测规则、情报、脚本程序，加固主机安全防线，实现主机威胁响应的闭环。

Agent 性能监控： 采集系统对自身性能和资源消耗进行实时的监控，并根据业务系统的繁忙程度对 Agent 资源消耗进行动态调整，将对业务系统的影响降到最低，优先保证业务系统的运行和稳定。

3.2 检测系统

检测系统由输入模块、检测模块、输出模块组成。



输入模块：该模块负责与采集系统的对接，主要作用是接收来自采集系统的数据，对数据进行解析和标准化加工，将数据整理为日志数据和文件数据两大类，有利于后续检测模块针对不同类型数据采用不同引擎。同时将整合好数据推送到检测模块。

检测模块：数据经过输入模块的加工后，会推送进检测模块，通过各类检测引擎进行威胁检测。针对日志信息会有威胁情报检测引擎、行为规则检测引擎、机器学习模型检测引擎，通过追踪入侵事件的整个生命周期，全方面多角度地检测主机威胁。在最常见、最难以检测的威胁类型上进行检测能力的优化加强，包括反弹 Shell、后门类木马、主机提权、僵尸网络、挖矿威胁、勒索威胁、虚假内核、远控工具、恶意环境变量、漏洞利用、恶意进程、关闭检测工具等威胁类型。在这些威胁类型上真正做到低误报、低漏报。针对文件信息有微步在线自研 NGAV（Next Generation AV）检测引擎，第三方 AV 检测引擎，多方检测引擎共同查杀，发现全网威胁。同时用户在许可的情况下可以启用云沙箱文件检测，更深入更全面地检测可疑文件。两大检测模块在检测上无论是深度还是广度，都做到了业内前列水平，全力保证主机安全无忧。

输出模块：该模块负责原始信息和告警数据的存储和输出，系统会将检出信息和原始流量日志记录至本地 Elastic Search 存储模块，将文件相关信息存储到 Ceph 文件存储服务同时支持 Syslog 形式或 HTTP API 形式(需定制) 输出给第三方日志平台。

3.3 分析系统

分析系统由事件聚合模块、日志调查模块、配置接受模块组成

事件聚合模块：该模块从安全人员运维实施、分析溯源的角度出发，提供安全人员用于分析威胁事件的功能，包括事件聚合、威胁上下文分析、攻击全链路等分析功能，在分析溯源过程中，不仅能有充足的上下文信息作为分析判断依据，也能高效率地理清威胁事件全貌。并提供可视化溯源的相关功能，包括事件分析图、进程链溯源图等，更直观地、通俗易懂地展现威胁事件的来龙去脉。同时提供一键响应功能，检测到相关威胁可以快捷高效地控制对应终端主机，响应高效且可靠。

日志调查模块：没有足够多的日志数据就难以做到全面检测威胁问题，在分析溯源过程中也缺少相关判断依据。为此，OneEDR 会将全量日志数据从终端主机侧拉取到系统平台上，在系统平台上可以高效地检索溯源，且不影响主机相关业务。同时提供日志智能检索，支持快速筛选查询也可以支持灵活语法输入，满足不同运维人员对溯源分析的高效率要求。并提供日志 Json 输出和 API 方式输出，运维人员可以更自由更灵活地分析处理主机日志信息。

配置管理模块：该模块支持用户下发配置和命令，实现对终端主机的响应、运维和升级。支持远程安装版本包脚本、算法情报的持续升级、运维监控等，实现基础的运维管理要求。

四、交付方式

产品为私有化部署，Agent 支持一行命令安装。检测引擎服务器部署支持硬件交付和软件交付。

4.1 硬件交付

本产品主要应用于对接服务器主机海量日志等场景，为保证吞吐性能，默认情况下，建议使用硬件交付方式，硬件设备规格：

型号	OneEDR-A1100
支持容量	5000 台服务器的检测与日志分析能力
设备类型	2U 机架式，含导轨
设备尺寸	高 87.8mm 宽 448mm 深 794.4mm
处理器	双路 CPU，16 核，共 32 线程
内存	128 GB
磁盘	4 块 1.2TB 10K/SAS 硬盘
电源	550W 电源模块 （支持冗余电源，需在订单中注明）

4.2 软件交付

支持云主机、虚拟机方式，规格需求如下：

操作系统	CentOS 7.6
CPU	32 核
内存	128GB
磁盘	3 块 1.2TB 10K/SAS 硬盘
软件	内部或外部 yum 源

注意：

1、 受环境影响，软件交付可能无法保证性能达到用户要求；

2、 本产品将独占该系统，请勿在同系统中部署其它三方系统或软件；