进程流量防火墙

Process Traffic 0 Day Firewall

ZDFW

BLUE AISEC

非授信的流量无所遁形

系统级 0Day 无法逾越

版权声明

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属 Blue AiSec 所有，受到有关产权及版权法保护。未经书面许可不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。

信息更新

本文档仅用于为最终用户提供信息，并且随时可由更改或撤回。

适用版本

本文档适用于内部合作伙伴。

免责条款

根据适用法律的许可范围，按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。

期望读者

期望了解本产品主要技术特性的用户、研发人员、售前人员、代理商成员等。本文档假设您对下面的知识有一定的了解:

- SSH 与 HTTPS
- TCP/IP 协议
- 网络安全基础知识

- 文档信息

文档名称			
扩散范围	保密不扩散任何人	**文档版本号**	2.0

作者		**日期**	2023.12
初审人		**复审人**	

- 版本变更记录

时间	**版本**	**说明**	**作者**

目录

1 前言

Process Traffic 0 Day Firewall 简称 ZDFW 是一款 Linux 服务器高级威胁感知系统，由 XDP 下一代流量防火墙、进程防火墙和主机安全组成，专注未知攻击 0day 对抗，目标是彻底解决服务器安全问题。

产品全部可以内网独立运行，大量实战稳定可靠，默认安装不会影响系统。

1.1 安全现状

随着 Internet、移动互联网、云计算的快速发展，云时代已百花齐放，越来越多的企业将业务和数据都是实现互联网+及云上迁移，业务会以数字化的形态运转在服务器主机上。内外业务交互传统的固定防御边界越来越模糊，传统的安全产品已经不适应新需求。从日益新增的现代攻击威胁来看，数据中心网络南北向、东西向均呈不同规模快速增加。互联网环境下的服务器安全面临着全新的威胁与挑战，安全形势日趋严峻。数字化转型过程中边界服务器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，整个信息系统中高价值数据的将面临失窃和被破坏的风险。因此，服务器安全已成为数字时代公认的信息安全最后环节。

1.2 当前困境

服务器安全作为信息安全最重要的最后一道防线，其建设难度仍在加剧，主要原因习惯于传统边界安全架构建设，忽略主机环境安全建设工作，与此同时，新型现代攻击威胁，如无恶意文件攻击和无视合法系统工具的权限索取（PowerShell）等攻击手段的应用，使得主机侧的安全防护工作变得难上加难。

- **传统边界解决方案无法适配云时代**

面对混合云、云原生等新型架构的大规模应用发展，以容器、服务网格、微服务、Serverless 为代表的云原生技术，带来一种全新的方式来构建应用。这也带来了一定程度的复杂性和挑战性，尤其是传统的安全防护方案无法平滑适配云原生架构环境。

- **0Day 漏洞无法及时发现**

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，漏洞影响极大，可以覆盖全球 70%的服务器。根据 FOFA 系统统计显示，全球对外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。

- **无文件新型攻击，防护难度加大**

近年来，随着更加高明的新型攻击方式的应用，如 0day 漏洞攻击、无文件攻击等基于内存的攻击手段，传统的依赖文件落地后进行的 webshell 和二进制恶意代码检测手段逐渐失效，防守方的难度逐渐加大。从近两年的攻防演练来看，无文件成为攻击方手里的“王牌手段”，通过在内存中注入或二进制恶意程序，在执行后不会留下任何痕迹，使其难以被检测和清除，从而达到破坏系统、提升特权的目的。新型攻击方法的运用，使得（云）主机面临更大的安全威胁。

- **终端电脑漏洞防不胜防，传统杀毒模式失效**

目前多数攻击是利用系统管理员终端电脑的邮件、office 文档、社交软件、输入法等漏洞，钓鱼入侵了终端电脑，在作为跳板进一步登录服务器，防不胜防，而且此类攻击比重越来越大。其行为和系统管理员一模一样，传统的杀毒软件和 EDR 完全失效。

1.3建设思路

通过上述针对当前网络安全现状及服务器安全面临的困难，采用 Gartner 提出的 CWPP 理念，提出了以工作负载为中心的安全产品，旨在解决现代混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。

- **兼容云架构及传统架构**

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。

- **漏洞侧防护**

具备强大的未知漏洞风险防护能力，能够对系统漏洞和各种应用漏洞被利用后发起非法连接进行精准发现，并针对进程流量做出精准分析，对非授信进程启动进行阻止。

- **威胁检测**

具备强大的入侵威胁防御及处理能力，能够检测常见入侵行为进行检测，如病毒木马、网页后门、异常登录等，同时也能够检测到高级攻击行为，如无文件内存马攻击、web 远程命令执行攻击等，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。

➢ **进程流量管控**

基于内核对外联进程原始报文收集学习，具备 TCP/UDP 报文风险分析，支持专家干预，任何异常流量均可被捕获；对服务器有端口及无端口服务流量进行分析捕获 ip 来源，对各个来源 IP 按 XDP、DDOS、FIREWALL 各特点进行防护。

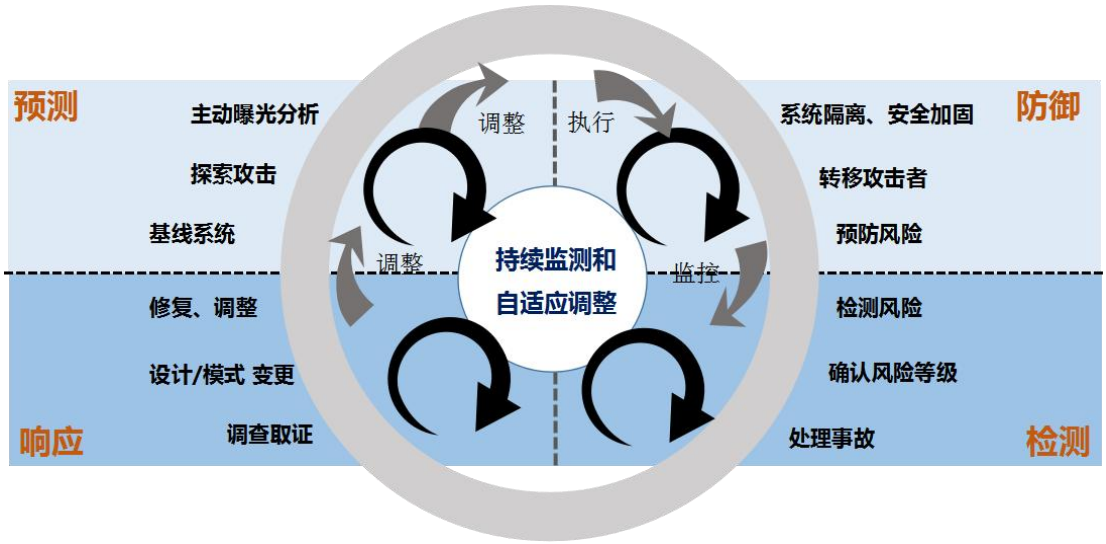
2 设计理念

采用先进的自适应安全架构、内核级进程分析及云工作负载保护平台（CWPP）解决方案，提供集中管理平台为用户解决私有云和混合云环境中可能遇到的各种安全问题。

2.1 自适应安全架构

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。大多数企业在安全保护方面，还是优先使用拦截和防御以及基于策略的防御控制手段将危险拦截在外，但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，自适应安全架构，有效解决传统专注防御手段的被动处境，为系统添加强大的实时监控和响应能力，帮助企业有效预测风险，精准感知威胁，提升响应效率，保障企业安全的最后一公里。

进程流量防火墙的设计架构采用自适应安全架构，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。



安全架构

2.2 Server 检测和响应

检测与响应，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及 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在其启动之初进行拦截。

server 检测及响应流程分为主机终端进程信息采集、威胁获取、AI 分析、告警及响应主要步骤。

2.3 CWPP（云工作负载保护平台）理念

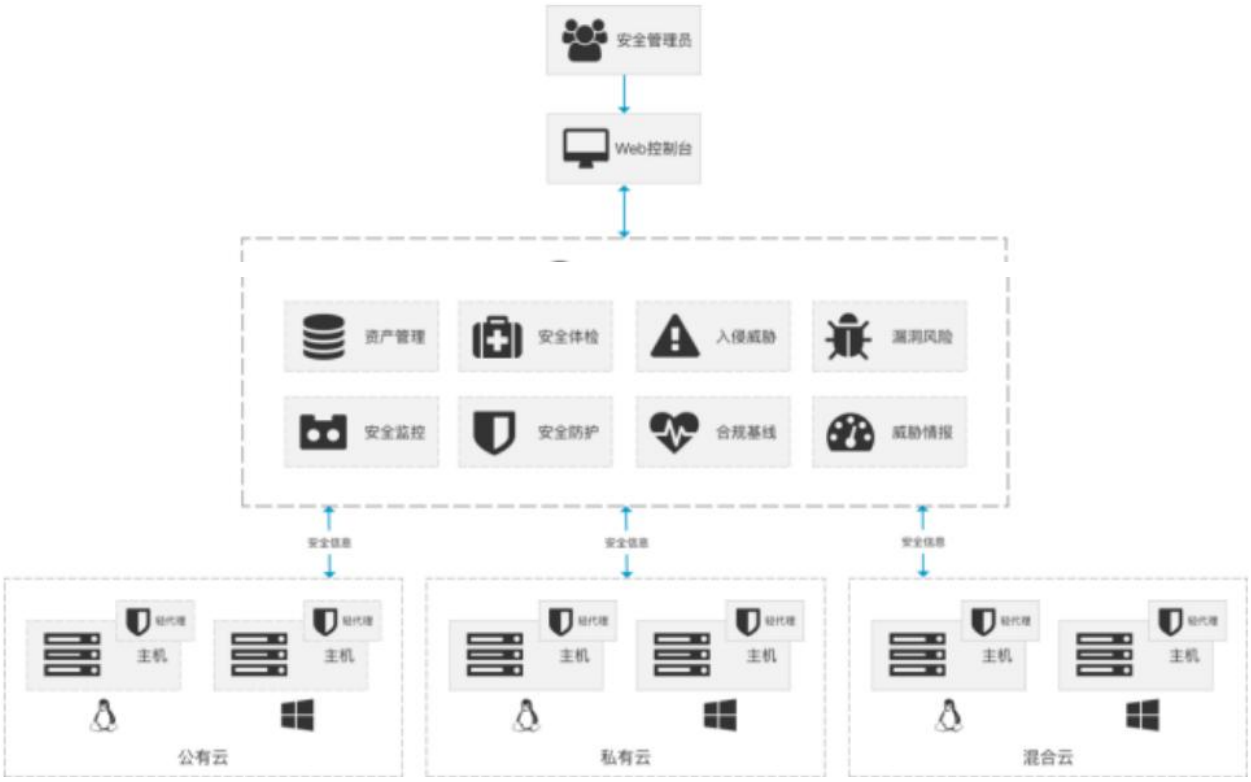
云工作负载保护平台（CWPP）的市场定义为基于主机的解决方案，主要满足现代混合数据中心、多云数据中心基础架构中服务器工作负载的保护要求。CWPP 应该不受地理位置的影响，为物理机、虚拟机、容器和无服务器工作负载提供统一的可视化和控制力，是云安全建设中首先要考虑的产品类别之一。

采用基于 Linux 内核技术的 Agent 解决方案，可以很好满足现代混合数据中心架构中服务器工作负载的保护要求，并且进程流量防火墙的产品能力基本覆盖了 CWPP 金字塔模型中的各个层级的要求。

3 产品概述

3.1 总体架构

进程流量防火墙平台，主要由端+控制台构成，提供了包含漏洞扫描、风险管理、入侵威胁管理、流量监控、安全防护、合规基线、抗 DDOS、安全告警、登录分析等功能。



换逻辑架构图

端：主机客户端轻量 Agent

客户端 Agent 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测和安全防护，可快速识别及阻断黑客攻击。Agent 主要功能：进程活动与流量分析并引入机器学习。

云：Server 端安全引擎

Server 端安全引擎作为平台的中枢，持续接收各个 Agent 上报的信息，并进行解析、处理、分析和保存，根据经验库和用户自定义规则，发现漏洞、异常登录行为、异常网络连接行为、文件异常操作、账号异常操作、异常命令调用行为和进程异常行为，实时发现入侵行为。

控制台：Web 管理平台

以 Web 控制台的形式和用户交互，清晰展示各项安全检测和分析的结果，并对重大威胁进行实时告警，同时以人机交互的方式提供用户自定义各种安全策略，以及灵活的策略分发，提升精细化管理，帮助用户更好更快地处理安全问题。

3.2 功能架构

物理安全：主要是监测计算资源使用情况，CPU、内存被进行消耗明细及风险预测。

流量安全: 基于各进程流量采集进行机器学习再综合分析, 可设置白黑名单、抗 DDOS、XDP 防护。

进程安全：捕获进程原始联网报文，在结合机器学习，对进程行为进行风控分析。

SSH 安全：分析 server 后台登录安全态势，以及操作命令记录，对公网服务器登录进行安全评估。

文件篡改：检测重要目录、重要文件是否被非法串改。

基线检测：对操作系统重要配置进程合规检测提高安全防护能力。

漏洞扫描：对指定文件路径进行扫描发现漏洞。

- **动态实时防护检测进程**

进程流量防火墙支持动态实时监控文件落盘的方式，检测在恶意文件篡改启动运行之前进行检测并处置，检测时效性强。而且支持自定义目录进行扫描和实时监控。

- **无文件内存马攻击检测**

内存马是无文件攻击的一种常用手段，通过在内存中植入恶意后门或木马并执行，达到远程控制 WEB 服务器的目的。在攻击者通过容器漏洞或应用漏洞注入内存马后，可在所访问任意 url 或者指定 url 中带上命令执行参数，进而在服务器执行系统命令。以 Java 为例，客户端发起的 WEB 请求可能会经过 Listener、Filter、Servlet 等组件，攻击者只要在这个请求的过程中在内存中修改已有的组件或者动态注册一个新的组件，插入恶意的代码，即可达到目的。

进程流量防火墙无文件内存马检测支持定时或实时检测注入进程的内存马，包括 Listener、Filter、Servlet 等内存马类型，并支持 JSP 和 Agent 注入两种检测引擎。

- **进程监控检测远程命令执行**

通过分析常见的远程命令漏洞利用实例，利用模式识别的方式，实时监控用户进程行为的各项特征，对主机中进程异常的执行行为和执行命令内容进行精确匹配，能有效发现黑客利用漏洞执行命令的行为痕迹, 并及时进行告警。检测的漏洞利用规则覆盖了 ATT&CK 攻击矩阵中 14 个阶段常见的攻击战术和 WEB RCE(远程命令执行) 漏洞利用的检测, 包括: 密码查看工具、提权工具、隧道工具、端口扫描工具、进程注入工具、计划任务、远程管理、获取交互式命令行界面、远程执行下载命令、白名单进程利用、0day 漏洞利用等等; WEB RCE 漏洞利用的规则包括：Java 反序列化远程命令执行漏洞、redis 远程命令执行漏

洞、IIS 远程命令执行漏洞、apache2 远程命令执行漏洞、php-fpm 远程命令执行漏洞及常见厂商的远程命令执行漏洞等。

功能同时也支持用户自定义规则进行检测，可帮助适应客户多样化的业务流程，精准覆盖各类 RCE 攻击的监控场景。

- **登录监控常用登录 IP 自学习**

进程流量防火墙支持自学习主机常用登录 IP，并记录到主机登录常用 IP 白名单中。白名单中的 IP 登录不告警。同时支持设置互信登录组，在同一个互信登录组内的主机相互登录默认为正常登录。

- **反弹 shell 检测**

通过对主机上的进程行为进行实时监控，识别进程的网络外联外联行为，实时发现进程的非法外联所产生的反弹 Shell 。支持查看反弹 shell 的详细进程信息，包括反弹进程信息、父进程信息、进程命令参数等。

- **异常日志删除**

本产品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。

- **文件蜜罐**

本产品支持文件蜜罐功能，支持对主机上的敏感文件设置规则进行实时监控，也支持创建虚假的蜜罐文件，来诱导黑客进行恶意篡改。支持监控的文件操作有创建、删除、修改、读取、权限修改，同时支持进程树的采集。一旦发现符合监控规则的恶意操作行为，立刻发送告警。

- **外联监测**

外联监测指通过机器学习主机外联行为，并形成外联行为基线，当检测到主机发生基线外的外联行为时认为存在异常外联，并进行告警。

3.3 合规基线

3.3.1 功能概述

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，通过使用本产品的合规基线功能进行基线检查即可轻松完成。

本产品对国家等级 2.0 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。本产品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。

3.3.2 特色功能

- **满足等保二、三级及 CIS 基线**

结合国家信息安全等级保护法规要求和 CIS 基线标准，不断推出满足等级保护二级、三级要求和 CIS 基线要求。

- **覆盖各类操作系统基线检查；**

目前产品支持常见的 Linux 系统的合规基线检测。

- **基线检测策略模式更全面更灵活**

基线检测任务支持配置任务的扫描机制以及适用范围，用户可以根据自身需求自定义检测模板，同时设置检测策略将检测模板应用于不同分组、不同标签的主机，实现灵活的基线检测策略。

4 关键技术

4.1 Agent 资源管控技术

进程流量防火墙在国内独家研发 Agent 资源限制自适应算法,用户可根据自身业务需求设置服务器安全 Agent 的资源控制策略，有效提高了 CPU 资源利用率，保障关键业务能分配到足够资源。基于该算法，本产品客户端 Agent 安在几乎涵盖所有传统安全防护功能的同时，还能做到单核 CPU <1%,峰值<3%。

4.2 采用轻量化 Agent 基座

进程流量防火墙采用插件化架构，Agent 作为大基座，轻量、稳定低消耗，功能通过插件进行扩展。采用插件化的架构，新增功能只需要单独开发新插件，无需更新 Agent 基

座即可实现企业不断演进的安全需求，通过管理平台将插件下发到轻量化 Agent 基座上执行即可实现安全功能灵活扩展。插件新增对原功能影响低，易于维护，同时每个扩展的新功能独立并存，互不影响。

4.3 非法进程防御

进程流量防火墙实时防御引擎采用实时监控进程的方式，对落盘的文件进行查杀。用户可自定义监控的磁盘目录，当目录文件发生新增、修改等变化时，本产品实时防护引擎捕获到文件特征，并对变化的文件进行扫描。

4.4 入侵攻击的主动检测

本产品凭借多年的技术积累沉淀，形成了成熟的网络层访问控制技术和操作系统层的内核加固技术，通过网络访问控制技术和内核加固技术，结合 ATT&CK 攻防技术，层层设防，可以有效检测和抵御来自网络层的攻击，以及有效检测系统层网络、账号、文件和进程的异常行为，并对异常行为进行阻断。

5 产品优势

5.1 轻量级 Agent

进程流量防火墙 Agent 采用插件化架构，插件化的 Agent 轻量、稳定低消耗，功能易扩展。采用插件化的架构，新增功能只需要单独开发新插件，无需更新 Agent 底座即可实现企业不断演进的安全需求，通过管理平台将插件下发到轻量化 Agent 底座上执行即可实现安全功能灵活扩展。插件新增对原功能影响低，易于维护，同时每个扩展的新功能独立并存，互不影响。

轻量化 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，其平均 CPU 消耗小于 1%，峰值可以自定义小于 3%。同时具备自适应降级和自适应熔断机制，减少 Agent 对业务的影响，确保业务优化原则。轻量化 Agent 安全、稳定和低消耗，安装部署无需重启服务器，以静默的方式自动执行，具备安全机制防恶意终止和卸载。

	CPU 占用	内存占用
普通状态	<1%	<30MB
峰值状态	<3%	<120MB

资源占用状态	Agent 自适应调节措施
当主机 CPU 平均使用率超过 50%且持续 2 分钟（可自定义）	Agent 自动降级,限制 Agent CPU 使用。
当主机 CPU 或内存平均使用率超过 90%（可自定义）	Agent 将会自动暂停工作

5.2新型高级威胁攻击检测

现阶段云工作负载面临的最严峻安全挑战是无文件攻击和内存马这一新型攻击策略。无文件攻击是指没有持久驻留在系统磁盘中的恶意代码攻击，攻击技术包括：内存木马、WEB 远程代码执行等。目前市场上的产品对这些攻击技术的检测与防御大多基于内核探针、RASP 等侵入性较强的检测技术。此类检测技术可致使系统在使用率达高峰时，业务连续性、稳定性受影响，且难以对无文件攻击做全面检测。

本产品的进程监控可实时采集监控进程流量，并跟据预设规则对实时数据进行分析与检测，可实时地针对 ATT&CK 攻击链各阶段的关键攻击手段做检测，能有效发现黑客利用漏洞执行命令的行为痕迹，并及时进行告警。

5.3兼容传统架构及云计算

本产品可以支持传统的 IT 架构，同时也支持公有云和私有云架构；并可以进行安全云管理。

5.4适配 Linux

进程流量防火墙同时支持各种类型的 Linux 系统。

本产品作为国内领先的云安全解决方案，坚持自主研发和国产化路线，积极推动产品与信创平台兼容适配。目前已实现对银河麒麟、统信操作系统 UOS、龙蜥、等主流信创操作系统以及 Redhat、、Centos、Debian、Suse 操作系统的兼容适配。经过严格测试，进程流量防火墙整体运行稳定，功能、兼容性等各方面表现卓越，可以满足用户需求。

5.5现联动响应

本产品支持将自身平台的资产数据、风险数据、告警数据等通过 API 和 syslog 的方式推送至第三方平台。同时本产品支持 api 接口与第三方平台（如安全运营平台）等联动，支持账户体系打通，还可以支持对本产品平台下发命令，如一键命令进行 IP 封禁、端口封堵。

6 客户价值

6.1 安全计算环境风险合规

网络安全等级保护基本要求 2.0 中，明确设备与计算安全相关的若干条款。安全计算环境作为内部防护的关键，承载着重要业务系统的运行，存储和处理着用户的重要数据，是保护对象的核心，进程流量防火墙在恶意代码防范、安全验证、入侵防范、安全审计、完整性监控等方面满足等保 2.0 的各项要求。通过细化等保合规相关风险配置检查项和合规要求，通过等级保护基线检查功能，提供主机层面一键式安全检查，助力企业内部等保合规相关要求自查及整改落地。

6.2 攻防渗透驱动最后一道防线建设

近年来随着攻防演练的不断开展，攻防技术水平不断加强，攻击方开始采取更为高明的新型攻击方式，因此企业尤其是涉及到关键信息基础设施的企业，正在加快构建企业安全防护体系，以应对每年国家和省市大型攻防演练活动。服务器安全逐渐成为了攻防对抗的新战场。

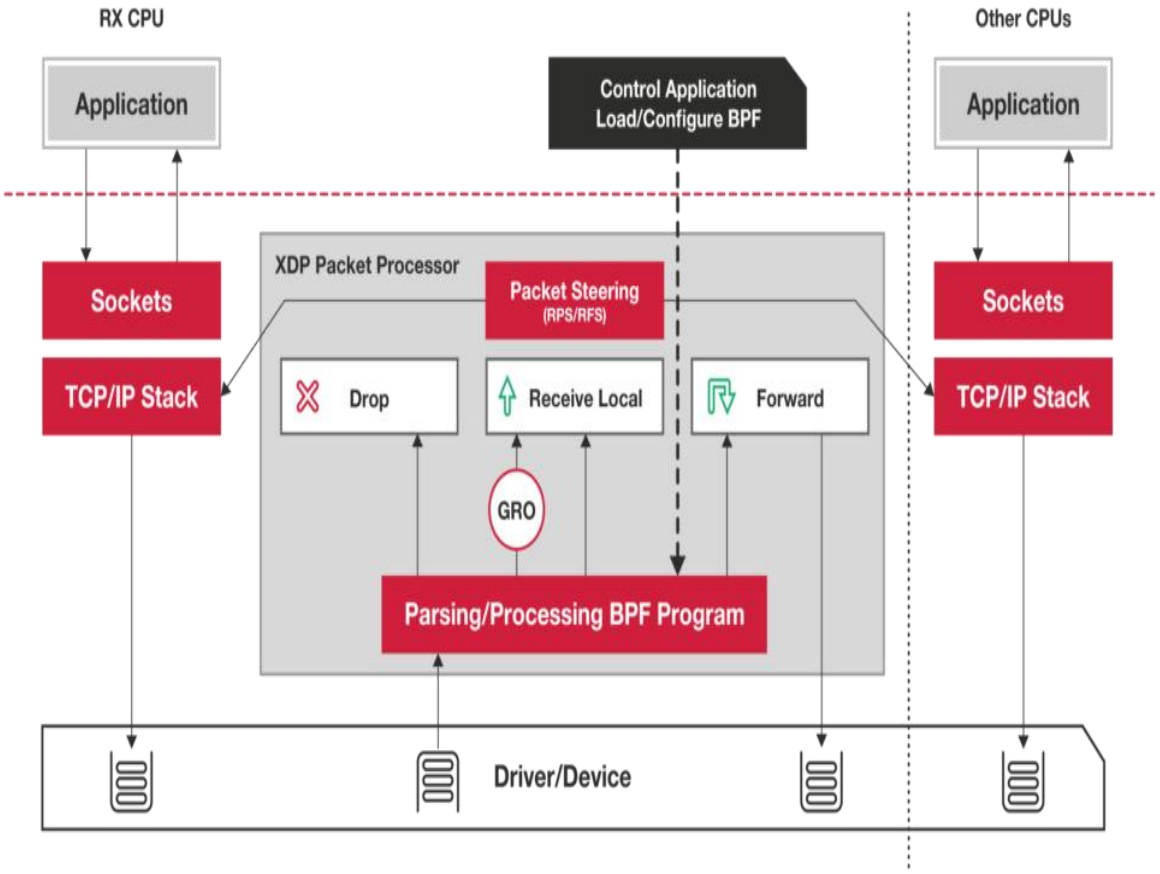
进程流量防火墙通过流量发现、风险分析检查等方式快速排查；基于主机进程通信、内存通信，内网异常行为发现能力，以及主机侧主动防御能力，构建主机侧安全防护体系。

6.3 未知攻击对抗

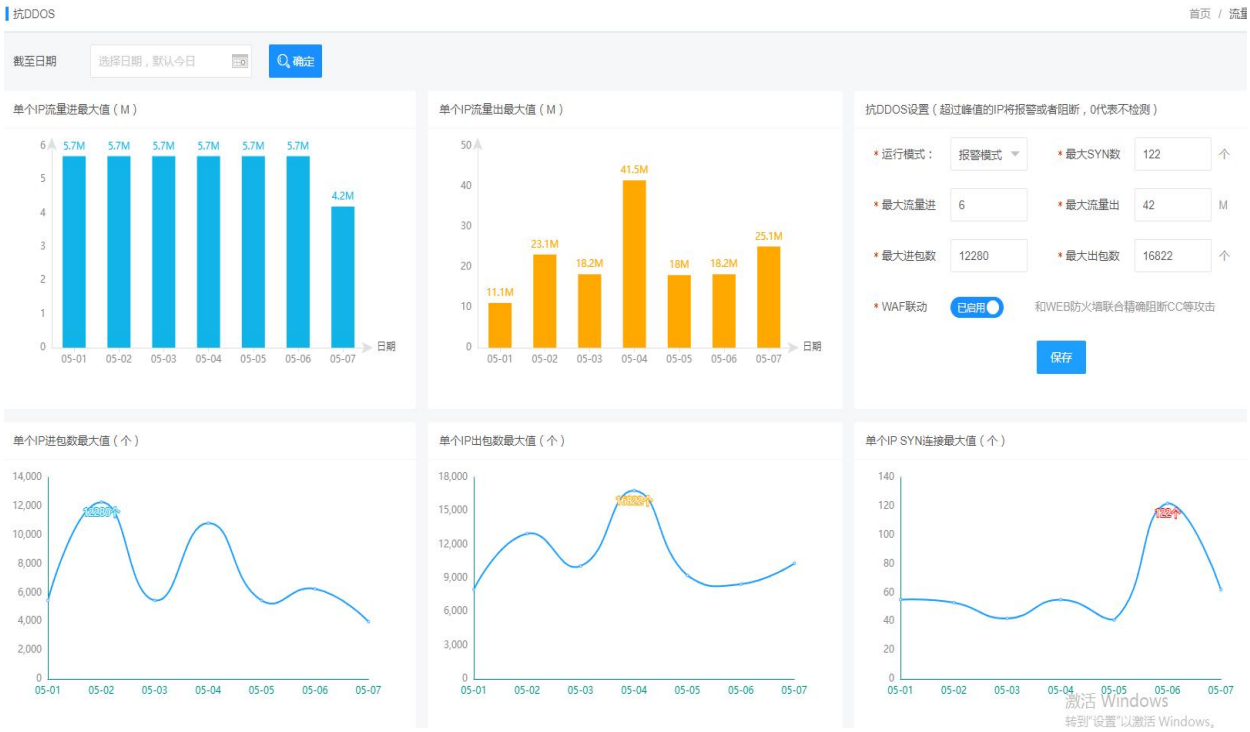
本产品具备全面的安全监控能力，从操作系统登录监控，文件和账号完整性监控，shell 命令审计，主机性能监控以及会话监控，进程行为监控，能够全面的对主机上的行为进行监控，记录主机上的一举一动，通过配置异常规则，快速发现异常行为。本质是全面对抗未知攻击威胁对抗，解决传统的杀毒软件、edr 等没有解决的问题。

7 部署方式

7.1XDP 流量防火墙



XDP 原理图



抗 DDOS 图

XDP 的全称是 eXpress Data Path，是新一代 Linux 内核中提供高性能、可编程的网络数据包处理框架，也是下一代高性能防火墙的标准，使得在服务器网卡层就可以进行高性能流量防御，其核心功能是 IP 流量过滤清洗和抗击 DDOS。

（1）通过流量深度学习根据 IP 地址流量进出等峰值，自动计算出最佳防御阈值，人工调整。

（2）可与应用层产品如 Web 应用防火墙联动，更加精准清洗 CC 等流量。

7.2 进程防火墙

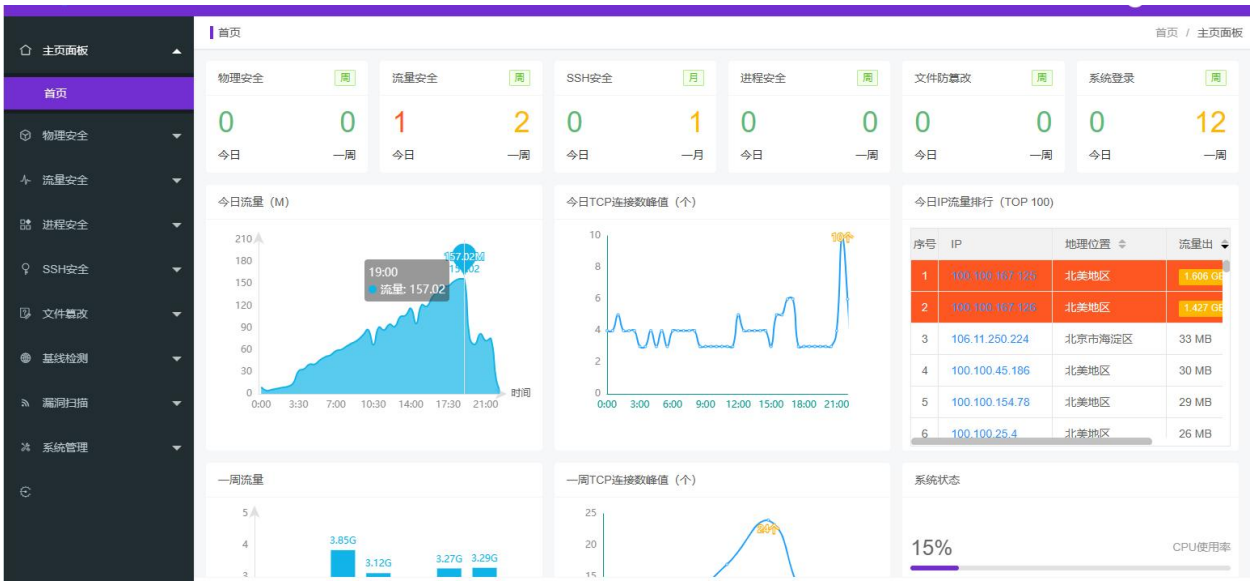
用机器深度学习检测每个联网进程的服务端口、访问 IP、流量进出、协议类型（TCP/UDP/ICMP）等，及时异常流量/木马等风险进程泄露数据。

（1）全程记录每个进程的 IP、进出流量、在线时长等数据。

（2）用 AI 技术分析危险进程，异地 IP/异常流量/危险行为等将报警。

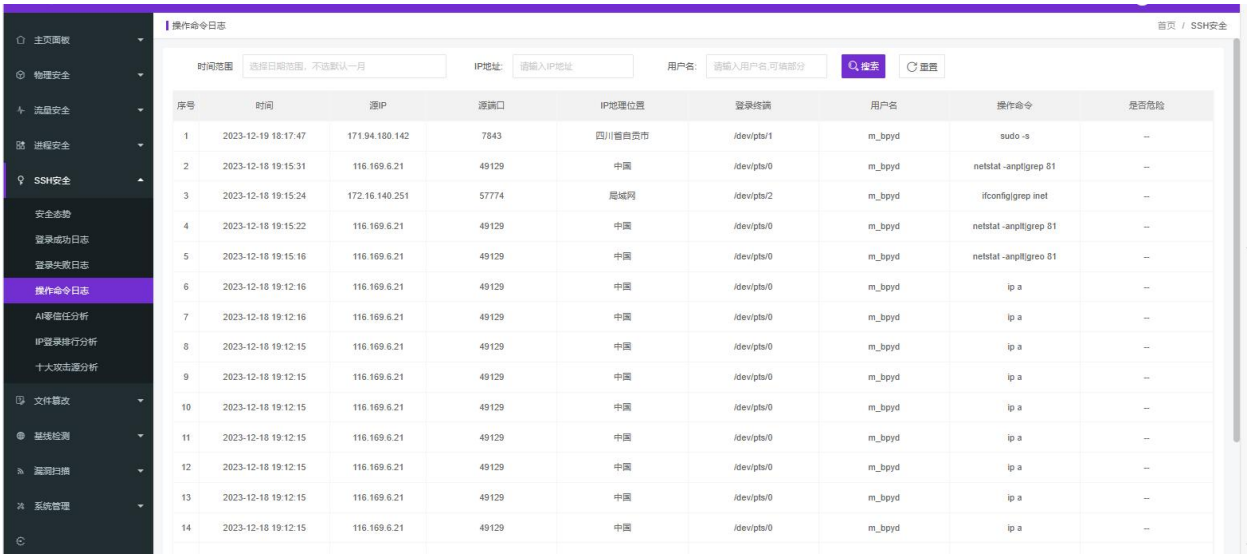
（3）黑白名单模式阻断进程，防止服务器被未知漏洞植入运行木马。

（4）全程记录各进程的原始报文，方便溯源分析，发现特别隐蔽的高级后门木马。



7.3 主机安全

包括物理安全、流量安全、文件防篡改、基线检查、SSH 安全、漏洞扫描等。其中对 SSH 登录做零信任，全面审计 root 用户和操作命令、及时发现系统管理员的终端电脑可能被黑客远控攻陷导致服务器被入侵。



组件漏洞扫描引擎 OSV-Scanner。

7.4 DEMO 地址

在线：http://47.99.142.2:9998/