八分量持续免疫系统

产品介绍

版本编号：v2.0

2020年04月30日

版本记录

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **日期** | **作者** | **修订说明** |
| **v.2.0** | 2020-04-30 | 八分量产品部 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1. 背景 2](#_Toc39942660)

[1.1. 政策背景 2](#_Toc39942661)

[1.2. 行业发展 4](#_Toc39942662)

[1.3. 名词解释 4](#_Toc39942663)

[2. 产品概述 6](#_Toc39942664)

[3. 功能介绍 7](#_Toc39942665)

[3.1. 可信防护 7](#_Toc39942666)

[3.2. 用户行为分析 8](#_Toc39942667)

[3.3. 主动对抗 9](#_Toc39942668)

[3.4. 区块链防篡改 9](#_Toc39942669)

[4. 行业解决方案 11](#_Toc39942670)

[4.1. 政务：泉州政务云 11](#_Toc39942671)

[4.2. 公安：某市公安局 11](#_Toc39942672)

[4.3. 银行：光大银行 12](#_Toc39942673)

[4.4. 证券：东吴证券 13](#_Toc39942674)

[5. 产品价值 14](#_Toc39942675)

[6. 未来规划 15](#_Toc39942676)

1. 背景
   1. 政策背景

2016年9月 《互联网信息安全系统使用及运行维护管理办法（试行）》

2016年11月 《中华人民共和国网络安全法》

2016年12月 《国家网络空间安全战略》

2017年5月 《网络产品和服务安全审查办法（试行）》

2017年7月 《关键信息基础设施安全保护条例（征求意见稿）》

2018年6月 《网络安全等级保护条例（征求意见稿）》

2018年11月 《互联网个人信息安全保护指引（征求意见稿）》

2019年5月 《关于加强工业互联网安全工作的指导意见（征求意见稿）》

《网络安全漏洞管理规定（征求意见稿）》

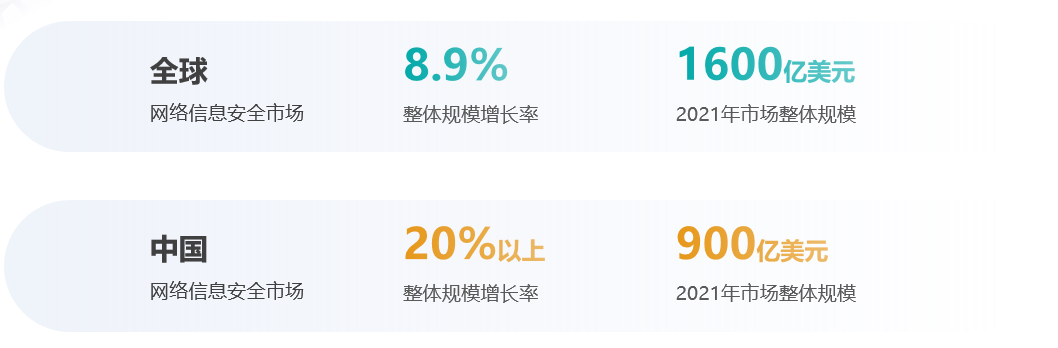
2019年6月 《网络安全等级保护基本要求》、《网络安全等级保护测评要求》、《网络安全等级保护安全设计技术要求》、《数据安全管理办法（征求意见稿）》

近年我国网络安全事件频发，国家及企业层面的信息安全威胁不断提升，国家网络安全政策也随之密集出台。

我国网络安全相关政策布局正在不断提速。腾讯生态安全中心2019年发布的《中国产业互联网安全发展研究报告》显示，截至2018年，国家22部委出台法律法规近200部，促进产业互联网安全发展。与此同时，地方政府也在加大网络安全产业扶植力度，例如北京市正在加快推进国家网络安全产业园建设，天津市则将推进网络安全产业、保障数据安全列为天津市发展数字经济的重要方向之一。《报告》预计两年内，中国网络安全将形成千亿市场。

2020年4月27日，国家互联网信息办公室等12部门联合发布《网络安全审查办法》。根据《办法》，关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查，该《办法》将于2020年6月1日起实施。

* 1. 行业发展



2019年全球网络信息安全市场整体规模达到了1382.8亿美元，同比增长8.90%，预计未来三年，全球网络信息市场规模仍将持续增长，至2021年，市场规模将超过1600亿美元。中国网络安全市场发展速度相比全球安全市场更为迅猛。增长率为20%以上，随着数字经济的发展，5G网建设的逐步推进，网络信息安全作为数字经济发展的必要保障，其投入将持续增加。预计未来三年，行业增速加快，到2021年,中国网络信息安全市场规模有望突破900亿美元。

传统意义的网络安全是伴生性技术，是伴随信息技术革新带来的一项技术应用分支。信息技术的持续革新变得越来越快，这不但会催生新的应用场景，也会促使一些旧的应用场景升级改造。例如云计算、云服务的普及，带来了人们工作和生活的巨大便利，随之而来的如何在云场景下做好安全防护成为新的需求点。区块链的日趋成熟，也在逐渐颠覆原有云计算的技术架构，新的技术变革已经到来。随着新兴数据（信息化）市场空间被进一步有效释放，信息系统的复杂程度将会越来越高，传统网络安全的技术局限性也将逐渐凸显，而这一局限性使其越来越难以适应技术变革所带来的新环境、新要求，传统网络安全面临着产业化发展的新挑战。这使得信息系统不得不寻求新的技术帮助，以解决越来越多的未知威胁。

* 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。 |
| **0day漏洞** | 安全补丁发布前而被了解和掌握的漏洞信息。 |
| **VM** | 虚拟机 |
| **HA数据库** | 高可用性数据库 |
| **API** | 应用程序编程接口 |

1. 产品概述

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、行为记录缺损等风险。一旦发生数据泄露，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？

持续免疫系统是一套安全管控平台，结合国际领先的可信计算、区块链与AI技术，对众多未知威胁进行早期智能分析，可以快速发现并提供辅助决策，有效抵御来自外部或内部的未知威胁和渗透攻击。

结合区块链技术的安全防篡改特性，实现关键日志的记录、防护、追溯等，从而使信息系统产生持续的安全免疫能力。

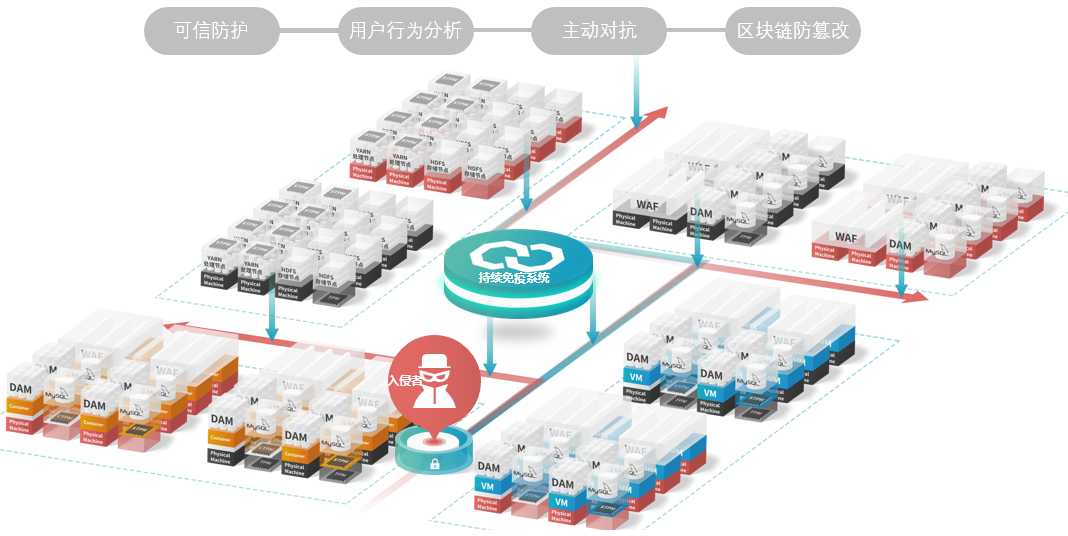


图2-1持续免疫系统

1. 功能介绍
   1. 可信防护

**功能描述：**

通过服务器可信状态白名单机制，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。从而极大程度地限制了入侵手段。一旦服务器的可信状态发生改变，可信防护系统可对异常进程自动进行阻断并发出警告，或者发出警告提醒管理员进行人工阻断。

服务器可信状态白名单可以通过可信防护系统分析该服务器的运维策略自动生成，也可以由运维人员人工导入。



图3.1-1可信防护

**产品优势：**

**白名单机制可在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：

**可信防护模块：**

* 可信硬件级别监控，对抗获得超级管理员权限的黑客；
* 可信环境1秒内告警，缩短攻击窗口；
* 细粒度白名单自动生成，降低管理复杂度。
  1. 用户行为分析

**功能描述：**

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

用户行为分析模块可基于已有的数据源生成相应的防御策略对用户行为或系统行为进行限制，管理员也可通过新建策略对用户行为或系统行为进行限制，当用户行为或系统行为出现异常时，及时发出警告。

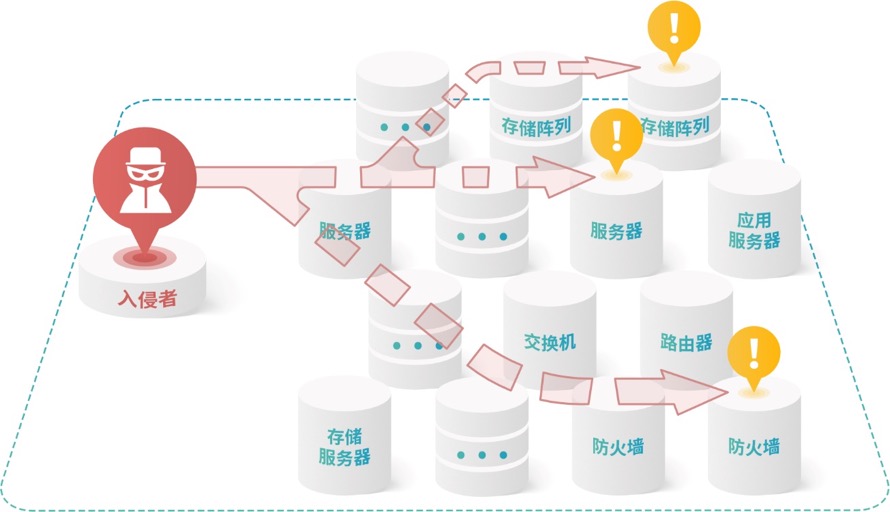


图3.2-1用户行为分析

**产品优势：**

**UEBA技术可在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：

**用户行为分析模块：**

* 依据大数据管理员行为画像，迅速识破盗用者异常操作行为；
* 精准过滤异常进程，极低误报率；
* 系统层操作行为分析，捕捉最细微的操作。
  1. 主动对抗

**功能描述：**

在人工智能技术的支持下，针对所感知、预判的威胁自动制定主动对抗策略，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。

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。

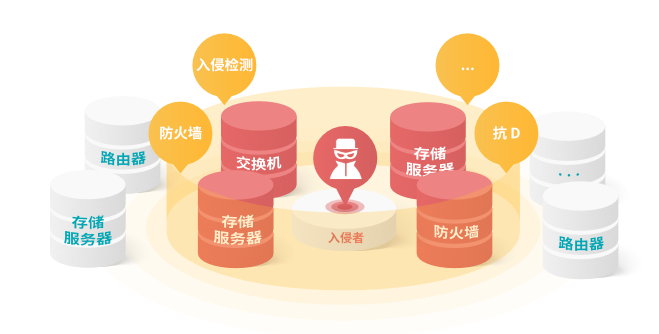


图3.3-1主动对抗

**产品优势：**

**人工智能技术可在15秒内自动部署对抗措施**

在告警触发到应急预案实施的时间窗口内：

**主动对抗模块：**

* 人工智能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，为安全管理员赢得时间；
* 智能生成威胁情报，辅助安全管理员快速决策。
  1. 区块链防篡改

**功能描述：**

利用自主研发的可信区块链技术，保障所有链上数据不被篡改。一方面，即便获得了最高控制权的外部入侵者，也无法抹除其攻击痕迹；另一方面，即使是内部高级管理员，也无法抵赖其违规行为，从而实现有效防范内外部攻击。

针对用户行为、安全威胁记录，该系统实现了数据的永久存证、防篡改以及可追溯。

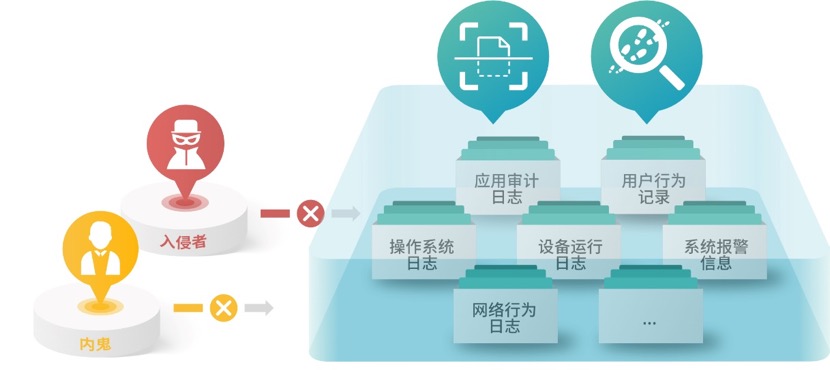


图3.4-1区块链防篡改

**产品优势：**

**可信区块链技术可实现永久存证链上数据**

当入侵者试图抹除系统日志以逃脱追责：

**区块链防篡改模块：**

* 区块链系统行为存证，比特币账本级别的防篡改强度；
* 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，恶意行为追溯，永久存证。

1. 行业解决方案
   1. 政务：泉州政务云

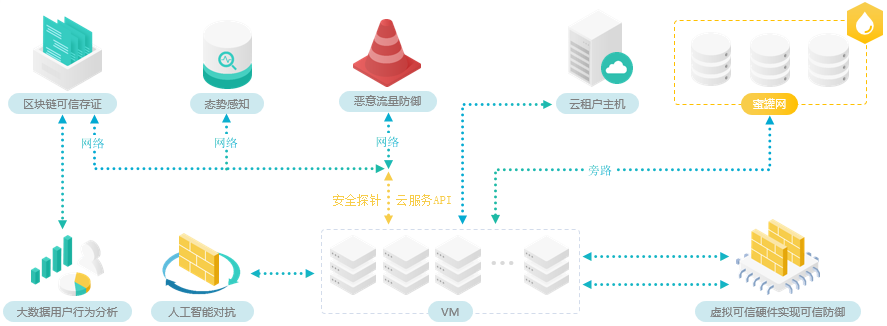
****

图4.1-1泉州政务云

当前新形势下，对政务云在网络安全性、合规度、社会公信力等多方面提出更高的要求，当前方案中提出的功能，充分运用区块链、人工智能和可信计算技术相结合，打造与时俱进的新型政务云平台，实现了：

* 政务工作智能化程度提升，有效降低安全工作的人力成本；
* 信息系统合规度高，满足政务云安全和等保等一系列法律法规要求；
* 业务流程完整追溯，便于监管追责。
  1. 公安：某市公安局

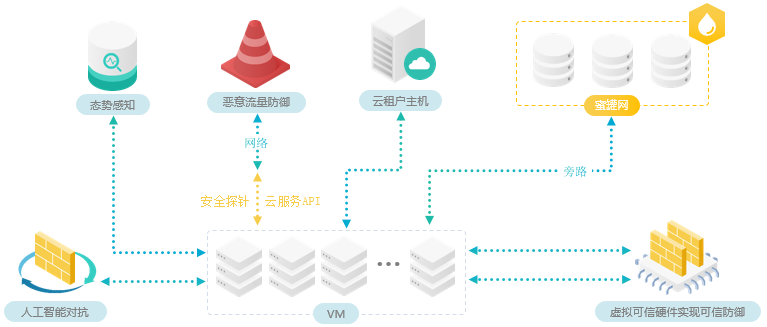
****

图4.2-1某市公安局

随着公安信息化向“大整合、高共享、深应用”的方向快速发展，公安信息的资源种类和数据量级激增，公安网内数据的集中存储和管理存在数据泄露、越权访问等诸多安全问题，通过在公安网络中实施持续免疫系统建设，实现了：

* 规范内网人员操作行为，严格的登录认证，结合用户行为分析技术，实现对用户行为的严格管控；
* 重要数据、日志等，永久存证，防止数据篡改等恶意行为；
* 在发生威胁时，启动智能防护进行自主对抗，确保网络信息安全。
  1. 银行：光大银行

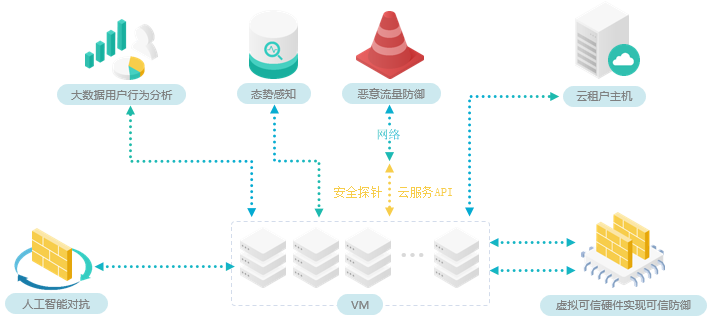
****

图4.3-1光大银行

随着云技术的发展，各大银行已经将信息系统迁移至云环境中，云上安全威胁随云扩展，传统安全方法和手段已经难以应对全新架构的云上安全问题，当前方案中提出的功能，实现了：

* 有效提高云端业务系统的安全性，为云计算平台及其承载的业务系统提供数据安全、应用安全、系统安全等多层次的安全防护；
* 从已有的用户画像和报警信息的处理等数据，采用AI的训练和加载，生成新的用户画像，使得系统不断适应业务需要；
* 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。
  1. 证券：东吴证券

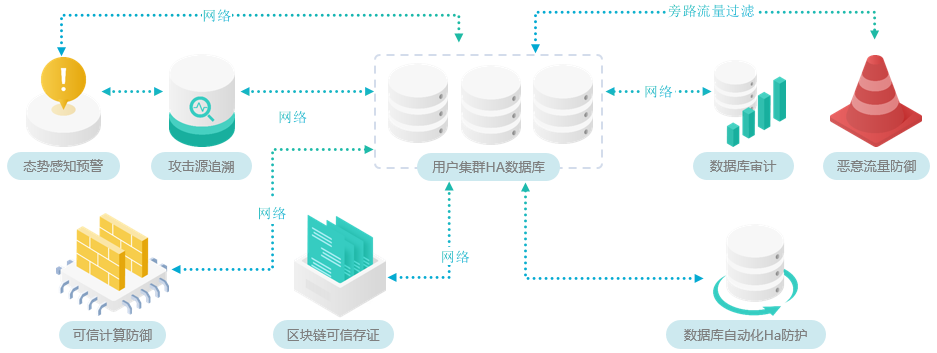
****

图4.4-1东吴证券

当前证券行业存在日志无统一查询和归档的问题，当前方案中提出的功能，通过区块链、大数据分析等技术手段有效保证了日志的真实性和准确性，建立统一的日志查询平台，实现了：

* 对券商端上传的日志进行真实性校验并将实时的校验信息上传到区块链，确保上传日志内容的真实性，有效杜绝日志被篡改的风险；
* 对于行业归集后的日志，可以相对独立地对日志内容进行大数据分析，对可能存在的交易风险进行监管分析；
* 根据监管的统一要求做日志查询，为行业监管提供了完整、统一、高效、准确的日志审计平台解决方案。

1. 产品价值

**快速部署**

* 轻量级、重实效的设计理念；
* 快速部署实施，确保企业终端不受影响；
* 快速搭建高效防御体系。

**持续监测**

* 持续监测与分析系统运行情况；
* 可发现来自不同权限用户的威胁。

**秒速响应**

* 面对未知威胁，第一时间发现恶意程序加载；
* 自适应处置、快速反应、最大程度降低风险。

**攻击可视**

* 直观展示异常行为；
* 安全警报、威胁情报一目了然；
* 帮助客户迅速判断决策。

1. 未来规划



在未来的发展规划当中，八分量会将可信计算、人工智能、区块链、5G技术深度融合，在可信计算技术的基础上，打造基于5G技术的安全体系架构；借助人工智能技术提升持续免疫系统的智能化、自动化程度；运用区块链技术，实现数据的安全存储、数据隐私保护和数据加密共享。将多种技术相结合，更好地实现防范内外部攻击、智能对抗各种威胁、关键数据防篡改和追溯等功能，构建全新的安全生态系统。