案例 1

北京天融信网络安全技术有限公司

面向高精端制造业的工业互联网平台安全综合防护体系

安全赋能助力产业发展

引言：

北京天融信网络安全技术有限公司（简称天融信）创始于 1995 年，是中国领先的网络安全、大数据与安全云服务提供商。自成立至今为工业企业和工业互联网平台企业提供了大量优质的解决方案，覆盖电力、轨道交通、航空航天、军工、能源、石油化工、机械制造、国防工业、汽车、电子等行业领域。

工业互联网平台是工业互联网产业发展的基石，安全是国家深入推进“互联网+先进制造业”的重要保障。工业互联网代表着国家新一代信息基础设施的重要发展方向，已经成为工业体系的神经中枢，提高工业互联网平台的安全体系建设，可促进我国工业互联网产业的加速发展。

天融信工业互联网平台安全防护体系从防护对象、防护措施和防护管理三大视角同时出发，构建完善的工业互联网平台安全框架。明确防护对象是前提，部署安全防护措施是关键，落实安全防护管理是重要保障。从工业互联网平台安全建设角度出发，强调技术与管理相结合、动静互补，全面持续提升工业互联网平台企业的安全防护能力。

一、项目概况

本方案基于工业互联网平台安全技术所开展的网络安全解决方案设计和综合安全防护体系建设，切实解决企业工业互联网平台面临的计算环境、数据安全、

访问安全、容器安全、微服务安全等安全问题，对工业互联网平台产业发展具有重大意义。

1. 项目背景

在当今以大数据为核心的工业互联网时代，没有安全就没有一切，网络安全上升为核心产业，这一领域将有超出想象的巨大的发展空间。我国高度关注互联网安全的新形势。中央领导从总体国家安全观的高度指出，安全是发展的前提，发展是安全的保障，安全和发展要同步推进。在工业互联网时代，网络安全至关重要，企业必须高度重视工业互联网平台安全问题，加强自身的安全威胁抵抗能力和防护手段。

2. 项目简介

本方案的建设实施，有助于供应链资产监控和风险预警，以及平台安全风险防范，大幅提升企业工业互联网平台安全防护能力，通过建设安全保障体系、提供安全服务保障平台业务流程安全，保障供应链完整，从而保障工业企业运营；大幅推动工业互联网平台产业发展，通过打造工业互联网平台纵深安全防御体系，为后续工业互联网平台安全防护体系项目建设竖立标杆，为引导和推动产业发展起到良好的示范作用。

2. 项目目标

本方案面向某高精端制造业工业互联网平台企业，围绕工业互联网平台边缘层、平台层、应用层及相应的业务处理流程和控制流程面临的突出安全风险，应用工业互联网平台安全防护核心技术，形成抗 DDoS、虚拟机逃逸、镜像篡改、数据窃取与篡改、恶意代码防范、身份认证、APP 检测等综合安全防护能力，提升工业互联网平台企业自身安全防护和态势感知能力。

二、项目实施概况

本方案充分贴合工业互联网平台的业务访问流程及控制流程，同时运用了业内比较成熟的安全方案以及针对性的新型安全解决方案。

1.项目总体架构和主要内容

工业互联网平台安全防护体系是基于工业互联网平台体系架构所进行的安全防护能力建设，其主要面向并贯穿整个工业互联网平台，从边缘层、平台层、应用层等多维度展开安全能力建设，边缘层与工业控制系统相关的控制设备，是企业生产的控制设备，该层主要实现对企业现场控制系统进行的安全防护；平台层是云计算环境以及工业大数据，是对边缘层的工业数据的处理，该层主要实现对工业大数据计算环境的安全防护；应用层为工业 APP 运行层，主要为开发者提供接口平台，以及企业用户实际应用的平台，该层主要实现对工业各类应用进行的安全防护。

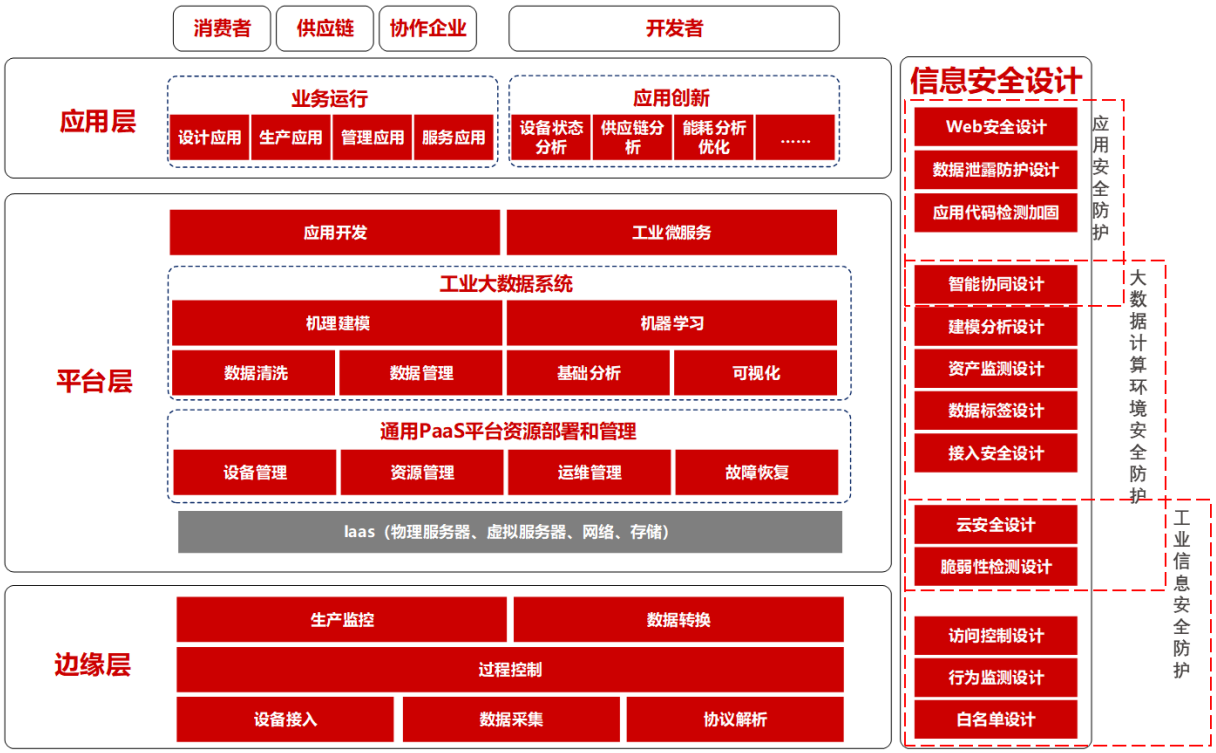

图 1 工业互联网平台业务框架

2. 网络、平台或安全互联架构

工业互联网平台安全综合防护体系安全架构呼应层次化防护架构，面向“边缘、平台、应用”构建“边缘计算防护、平台应用防护以及安全管理中心”三个层面的安全架构。

边缘计算防护注重设备安全、控制安全及网络安全三方面能力，形成包括协议深度解析、基于行为内容访问控制、边界隔离、接入认证以及通讯加密在内的安全能力；

平台应用防护注重网络安全、应用安全、数据安全三方面能力，形成访问控制、抗 D、恶意代码防护、统一用户管理、云计算安全、应用加固、数据防泄漏、数据脱敏、大数据安全等安全能力；

安全管理中心利用大数据分析技术对海量安全数据进进行采集、清洗、归一，结合规则库、地址库、威胁库进行包括关联分析、流式分析在内的安全分析工作，最终向用户实现包括资产管理、事件管理、安全审计、风险识别、态势展示、事件告警、安全处置及数据治理在内的安全应用交付能力。

图 2 工业互联网平台综合防护体系框架

3. 具体应用场景和应用模式

基于工业互联网平台的安全应用场景下，实现以下不同安全层面的应用模式，构建的纵深防护体系：

- **面向边界场景**

对工业互联网微服务平台边界采用访问控制隔离技术手段，对设备的接入实现准入认证，在边界实现企业用户的访问控制以及设备的访问控制安全能力，做到设备安全入网、边界防入侵、防攻击的安全能力保障。

- **面向平台业务和应用场景**

在工业互联网平台业务和应用的连续性、完整性等层面，对于数据泄露、篡改、丢失等问题进行业务和应用层面的安全能力保障。

- **面向大数据的场景**

对工业互联网平台的海量工业大数据的设备数据、业务系统数据以及访问用户隐私敏感等数据内容，在采集、传输、存储、处理等环节采取数据加密、访问控制、数据脱敏的数据安全能力保障。

- **面向云基础设施场景**

对工业互联网平台的云计算环境中的物理服务器、虚拟主机、容器、虚拟化网络进行二到七层不同租户的不同安全能力灵活划分，满足云环境下的定制化、可扩展的不同安全防护要求。

4. 安全及可靠性

设计贴合等级保护 2.0 的相关技术要求，符合“一个中心、三层防护”的安全原则。并且安全建设本身要符合平台的业务处理流程及控制流程。项目实施方案充分考虑了平台的业务处理流程及控制流程，首先通过定制化的平台安全产品及定制化的云安全、容器安全产品满足“安全区域边界”、“安全通信网络”、“安全计算环境”的要求，最后通过 APT 防护及安全态势感知进行上层的统一安全管理，综合建立成行业化、定制化、场景化极高的工业互联网平台安全综合防护体系。

5. 其他亮点

（1）提出了一套具备创新性的工业互联网平台企业安全态势感知架构

包含数据收集、存储、分析、展示，对平台中存在的攻击行为进行统计和挖掘，对工业互联网平台安全态势进行整体感知，其功能架构设计和应用代表了平台建设过程中的创新技术能力。

（2）采用创新的规则库持续更新技术

通过搭建安全防护平台，可以获得工业互联网平台中存在的安全漏洞、恶意代码程序等信息，这些安全信息一旦被发现将被用于网络安全研究，并在实验环境中进行验证，以获得更多的安全技术研究素材，并经过开发测试后作为安全防护产品的规则库升级补丁，为平台持续提升安全防护能力起到重要作用。

三、下一步实施计划

1.优化防护策略，实现协同动态防护

根据工业互联网企业的业务流程，及时调整部署在企业中的安全防护设备的策略配置，应用工业互联网态势感知平台实现安全持续监测、威胁情报收集及网络安全态势实时展示，将感知层获取的信息进行深度分析，制定相应策略并自动下发，驱动各种安全引擎做出动态调整，从而实现更为智能、快捷和有效的安全防护和感知，构建工业互联网平台企业协同动态防护体系。

2.推广应用

（1）借助标杆案例向同行业其他企业推广

本解决方案服务对象为支撑供应链产业发展的工业互联网平台企业，此类平台企业是工业互联网平台未来的发展趋势。本解决方案充分贴合工业互联网平台特点，可以作为整个工业互联网平台企业综合安全防护系统标杆案例向同行业其他企业全面推广，供其他企业参考作为网络安全解决方案。

（2）面向产业聚集区、示范区、工业园区推广

产业聚集区、示范区、工业园区是供应链产业的主要载体，本解决方案以供应链平台企业为服务对象，作为供应链中重要的一环，其推广有利于推动供应链产业的发展，为产业链稳定安全运行保驾护航。

（3）面向不同行业的工业互联网企业推广

本方案应用了先进的安全防护技术和成熟的安全防护产品，可推广应用到不同行业的工业互联网企业，更好的发挥产品和解决方案应用价值，为工业互联网企业构建全方位的安全防护体系，实现良好的防护效果。

四、项目创新点和实施效果

1. 项目先进性及创新点

（1） 项目先进性

- 可视化数据建模技术

平台的多维数据分析功能都是基于多维分析技术来实现。多维分析技术通过对业务数据的充分理解，首先通过数据索引建模技术完成数据仓库的构建，然后在数据仓库基础上利用统计、关联、挖掘等分析手段为构建数据分析模型、数据分析任务，然后通过数据分析任务执行输出分析结果。

- 先进的事件归并技术

平台的事件归并技术可以根据用户指定要归并的信息的特征、字段等信息进行归并，只有具有该特征、字段的信息才可以被归并，即当多个信息的指定特征、字段的内容一致时，产生一个归并信息。同时，用户可以自己指定是否丢弃原始信息。

- 基于状态机的实时关联检测技术

平台通过基于状态机的实时关联检测技术使用状态机来抽象和描述攻击的过程与场景，状态机间的状态转换的条件由不同安全事件触发。同时，实时关联分析技术通过对事件的关联，可以有效的帮助我们过滤事件，在大量事件（甚至是误报事件）中提取有用的信息。

- 基于微内核节点管理技术

平台中数据采集层、数据汇聚层涉及的所有节点均使用统一的节点技术。该节点技术采用了微内核架构，将核心功能与业务服务功能进行了剥离。支持以组件的方式扩展节点的业务功能；支持定义组件间的数据依赖关系及执行顺序。节点支持多级分布式部署，可适应复杂的网络部署要求。以容器的方式对各组件进行管理，提供在控制端对各组件的远程配置管理及应用升级。

- 监测技术

APT 监测技术能够对特种木马等恶意代码的虚拟机探测技术进行检测和处理，避免恶意代码的绕过，并支持反虚拟机检测。

（2） 创新点

- 采用创新的分布式文件存储及检索技术

可横向扩展，支持高达 PB 级的数据存储及检索，支持十亿级别数据秒级检索响应。

- 采用基于单机流程与容器算子的双层调度控制技术

单机流程负责模型整体流程控制，支持跨计算框架的复杂计算模型，容器算子负责控制在同一计算框架内运行的模型，可以最大限度的优化模型的执行效率。

- 采用面向数据流程的算子建模技术

按数据流程可分为：输入、处理、分析及输出四类算子，采用开放式算子接口，并支持第三方扩展。

- 采用创新的攻击轨迹技术

向用户提供根据攻击线索信息追溯到的更多攻击相关信息，包括但不限于攻击发生的时间范围、进展过程、攻击者信息、利用的漏洞、使用的工具等信息。

2. 实施效果

工业互联网平台企业纵深安全保障体系主要实现公有云服务安全防护功能以及工业互联网平台内部安全防护功能。

（1） 公有云服务安全防护功能

对公有云服务存在的具体安全风险进行分析，从客户安全需求角度出发，运用虚拟化安全防护技术、攻击防护技术、接入安全防护技术等多项安全能力，构建工业互联网平台公有云服务安全防护体系。实现访问控制、接入认证、抗 DDOS 攻击防护、入侵防御、恶意代码防护、Web 应用安全防护等多项功能。

（2） 工业互联网平台内部安全防护功能

对工业互联网平台内部存在的具体安全风险进行分析，从客户安全需求角度出发，运用云环境安全防护技术、大数据和态势感知技术等多项安全能力，构建工业互联网平台内部安全防护体系。实现接入安全防护、大数据环境安全防护、数据安全防护、云计算环境东西向流量安全防护、云计算环境南北向流量安全防护、云计算虚拟机逃逸防护、容器安全防护、微服务安全防护、计算资源安全防护、APT 安全监测、平台态势感知防护等多项功能。

本解决方案帮助用户解决了工业互联网平台企业公有云服务中身份认证、数据流转、南北向流量分配等安全问题，以及平台内部云计算环境、数据安

全、东西向流量与访问控制、容器安全、微服务安全等痛点问题。并获得以下经济或社会效益：

- 带动产业链行业的产业升级，防范安全威胁，显著降低工业互联网平台企业面临的网络安全风险。
- 有利于相关行业标准的建设及孵化。
- 有利于国家相关部门对工业互联网平台信息安全态势的管控。