案例1

杭州安恒信息技术股份有限公司

主标题：基于 MSS 的工业互联网平台安全防护体系建设

副标题：安全托管理念的平台运营新模式，助力工业互联网安全服务向中小企业普惠开放

引言：随着工业互联网的快速发展，工业互联网平台作为核心，成为推进制造企业降本增效、加速转型升级的重要途径。平台服务商通常采用自建私有云、租用公有云或搭配使用混合云等方式建设工业互联网平台，实现自身与其他联网工业企业、服务商的工业应用与数据的上云、管理和数据的处理、分析和应用。然而，传统安全产品防护能力已不足以应对工业互联网新场景下的安全挑战，因此，建立一套低成本、全方位、多角度、有弹性、易维护的安全运营服务体系，成为众多工业互联网平台安全建设的首要目标。

一、项目概况

针对工业互联网平台存在的安全需求，安恒信息规划设计了一套基于 MSS 的新型工业互联网平台安全防护体系：将传统的工业控制系统信息安全、设备安全、网络安全、工业数据安全、工业云安全的能力进行资源化、服务化封装，形成按需分配、弹性扩展、高效可靠的安全能力资源池，实现了安全能力随需随取随用，并藉此构筑新型一体化安全防护体系，为工业互联网平台整体安全赋能。

1. 项目背景

工业互联网成为企业数字化转型抓手的同时，也面临着多种多样的网络安全问题，2019 年上半年，CNCERT 加强了针对联网工业设备和工业互联网平台的网络安全威胁发现能力，累计监测发现我国境内暴露的联网工业设备数量共计 6814 个，包括可编程逻辑控制器、数据采集监控服务器、串口服务器等。其中，存在高危漏洞隐患的设备占比约 34%。此外，CNCERT 监测了境内具有一定用户规模的大型工业互联网平台 40 余家，业务涉及能源、金融、物流、智能制造、智慧城市、医疗健康等方面，并监测到根云、航天云网、COSMOPlat、OneNET、OceanConnect 等大型工业互联网平台持续遭受漏洞利用、拒绝服务、暴力破解等网络攻击，工业互联网平台已经成为网络攻击的重点目标。

工业互联网平台服务商通常采用自建私有云、租用公有云或搭配使用混合云等方式建设工业互联网平台，实现自身与其他联网工业企业、服务商的工业应用与数据的上云、管理和数据的处理、分析和应用。然而，传统安全产品防护能力已不足以应对工业互联网新场景下的安全挑战，同时传统安全体系建设部署复杂、成本高、维护难。因此，建立一套低成本、全方位、多角度、有弹性、易维护的安全运营服务体系，成为众多工业互联网平台安全建设的首要目标。

2. 项目简介

针对上述业务场景下的安全痛点问题，杭州安恒信息规划设计并实施了一套基于 MSS 的工业互联网平台安全防护解决方案。该方案围绕工业互联网平台安全、应用安全、数据安全、网络安全、控制安全、设备安全，运用 SaaS 化、服务化的资源整合方式，形成按需分配、弹性扩展、高效可靠的安全能力资源池，并藉此构筑新型持续一体化安全防护体系，解决了工业互联网平台的云上业务系统安全问题。

该体系通过基于大数据和深度学习的智能风险预测技术，对工业互联网多层次安全风险要素进行集中分析和处理，实现安全模型在工业互联网场景的落地应用，依托 SaaS 化安全服务实现对所有工业互联网安全的“集中配置、统一管理”。同时方案创新性地采用了区块链数据隐私计算功能，保障了工业互联网数据的“可用不可见”，极大推动了工业企业上平台、用平台的积极性，保证工业互联网全产业链在数据安全、平台安全、应用安全、用云管云过程中的安全互联互通，提高了工业数据的流通价值。

3. 项目目标

平台围绕工业互联网平台安全、应用安全、数据安全、网络安全、控制安全、设备安全层面的突出安全风险，建设基于 MSS 的工业互联网平台安全防护体系。具体目标如下：

（1）构建 SaaS 化的工业互联网安全一站式服务平台

围绕工业互联网边缘层、工业 IaaS 层、工业 PaaS 层、工业 SaaS 层以及工业数据面临的安全风险，建设覆盖工业 APP 安全、工业云平台安全、终端安全、数据安全需求的一站式安全能力资源池。

（2）构建以用户为基点的全局安全审计体系

整合工业互联网平台终端、流量威胁分析、WAF、态势感知、防火墙等多个维度的数据，建立基于数字身份的全局安全审计体系，实时监测用户的访问和使用行为并进行合规性分析，准确监测识别出异常行为和安全威胁并及时响应，提升工业互联网平台的整体安全防护能力。

（3）建成工业互联网平台安全综合防护系统

以态势感知中心进行统一管理与监测，汇聚平台接入终端、网络基础设施、平台基础设施、工业微服务、工业 APP、防护设备等安全数据并进行综合分析，以 MSS 安全运营托管服务，实现业务应用在 7×24 小时内不间歇运行；建立工业互联网平台安全态势感知中心，对 95%以上范围的的信息安全防护设备，网络交换机、工作站、服务器、终端等设备，以及工业互联网平台流量等进行网络安全监测分析，形成工业互联网平台企业的安全统一管理与态势感知能力。

二、项目实施概况

本项目构建的基于 MSS 的工业互联网平台安全防护体系主要实现对工业互联网的设备接入安全、控制安全、网络安全、云平台及业务应用系统安全以及数据安全，并提供低成本的 SaaS 安全服务，解决工业互联网业务场景的安全问题，保障工业企业高效、稳定、安全地数字化转型。

1. 项目总体架构和主要内容

在现有工业互联网平台架构的基础上，针对工业互联网平台原有的传统安全架构思想重新评估，以 MSS 安全运营能力为核心，对某双跨工业互联网平台的关键服务进行隐藏保护。通过建立持续安全运营中心，实时、持续进行动态评估，结合动态访问控制、最小权限、信任评估机制，提升平台整体安全防护能力。

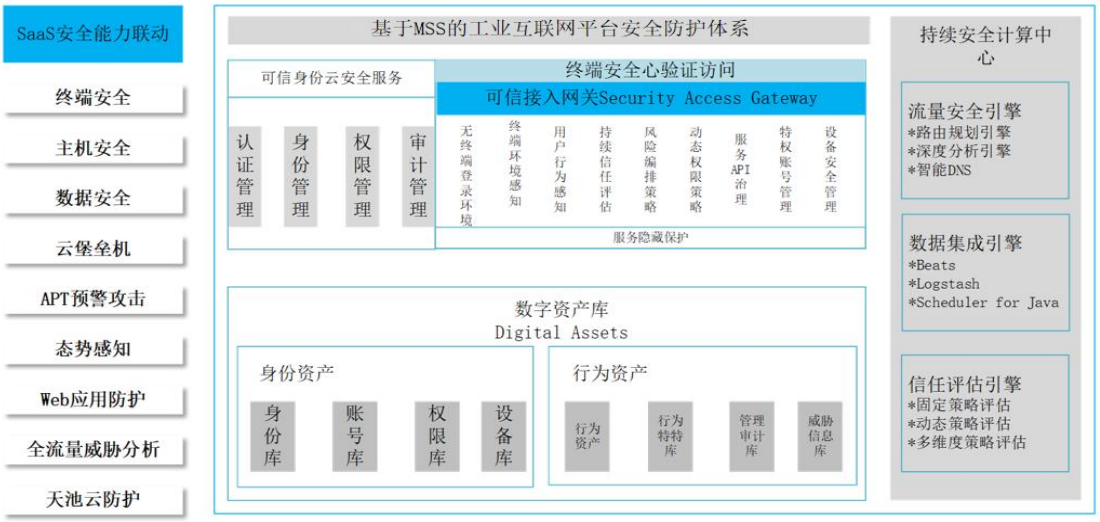

图 1　工业互联网平台安全能力架构图

（1）云安全体系建设

基于云计算安全防护思路，安恒信息以 MSS(安全托管服务)的创新防护模式，构建安全运营中心，形成了“运营+技术+服务”的云计算安全防护体系，从云租户、云平台、云安全运营层面降低工业互联网平台自身云平台和云租户面临的安全风险，实现云平台的安全持续性和合规性。

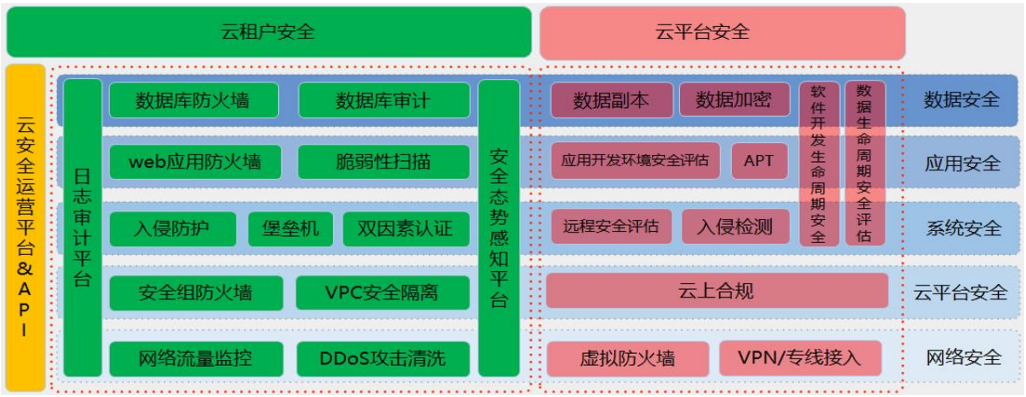

图 2 云安全体系能力全景图

（2）安全能力 SaaS 化

通过把安全运营 SaaS 化、安全防护 SaaS 化、安全管理 SaaS 化，基于云计算、工业互联网、大数据等核心安全技术，建立一套能够实现安全能力可扩展、有弹性、易维护的 SaaS 化立体纵深安全防御体系，实现对云安全能力的 SaaS 化

赋能。

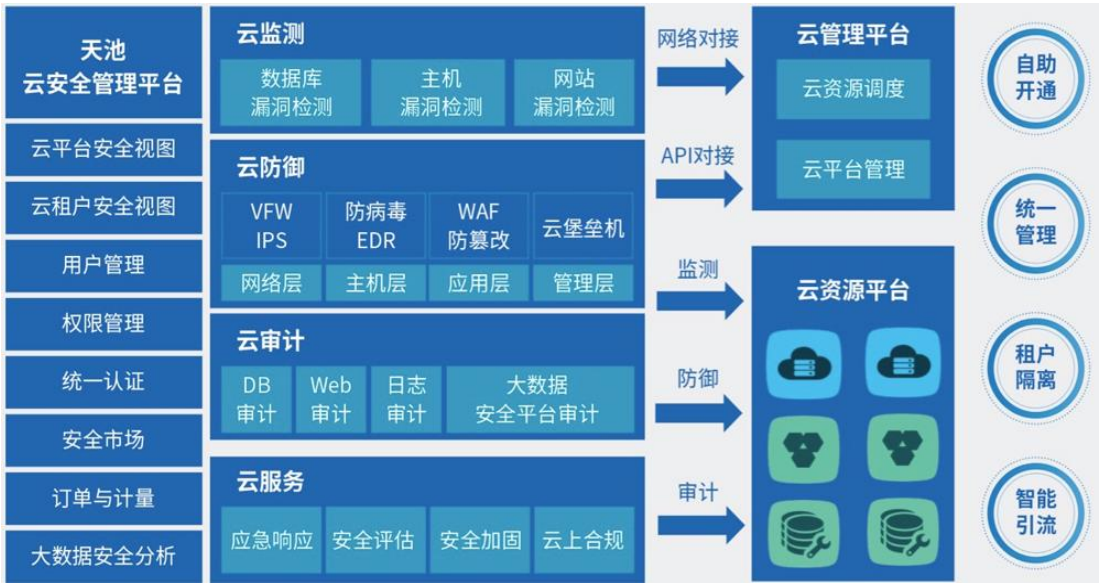

图 3 SaaS 化安全能力体系图

a. SaaS 化云监测服务

实现云化的 Web 应用弱点扫描、综合漏洞扫描、数据库弱点扫描、安全配置基线核查等能力。

b. SaaS 化云防护服务

提供网络流量检测防御、Web 应用防护、网页防篡改和主机安全及管理能力。融合下一代云防火墙能力，通过威胁情报、DDoS 防护、Web 防护、CC 防护、数据防护 5 大防护模块为云租户提供防攻击、防篡改、防瘫痪、防泄露等安全防护服务。

c. SaaS 化安全审计

实现云化的安全运维审计、综合日志审计和数据库安全审计能力。可对用户的各类日志进行综合审计分析，发掘潜在威胁，可追踪溯源；SaaS 化数据库安全审计可实现对进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原操作细节，迅速发现和响应数据威胁。

d. SaaS 化安全接入

在端侧和边缘计算处提供接入安全服务。以 SDK+API+开发指导文档的方式给联网工业企业提供数据安全传输保障；在厂侧设备、边缘网关内置安全心，对数据进行安全加密，对接入设备进行身份认证。

e. SaaS 化安全运营

对各种安全能力集中管理调度，结合大数据分析，为云租户提供安全视图，可对云资源实现整体安全感知。

（3）工业互联网数据共享安全

基于平台的工业大数据可信执行环境，配合安全调试沙箱、安全计算沙箱，身份认证和区块链合规审计等模块，结合密钥管理系统提供的统一密钥管理和加解密服务，在保障工业数据安全的同时，实现工业数据的可用不可见，可用不可取，充分保障工业数据的开放共享安全，最大限度发挥工业数据的潜在价值。

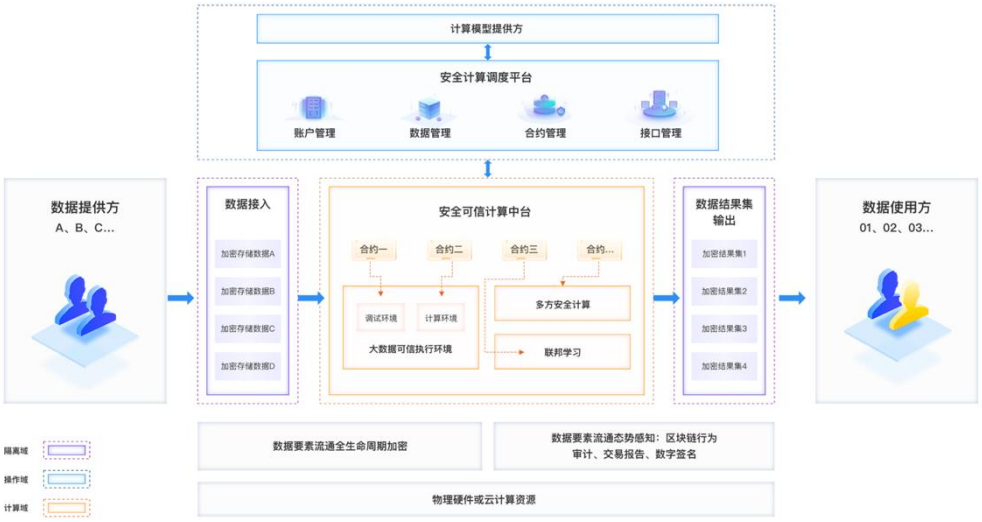

图 4 数据共享技术总体架构

2. 具体应用场景和应用模式

本方案可以在智能制造、建材、轨道交通、电力能源、市政水务等工业互联网领域普遍应用，保障工业企业在工业互联网业务场景下的设备接入安全、网络安全、控制安全、云平台及应用安全以及数据安全，构建基于 MSS 化安全防护能力及 SOAR 自动化阻断的运营能力，构建覆盖工业互联网安全事前监测、事中防护、事后响应的自动化安全服务体系，实现工业互联网的持续、稳定、安全运行。

目前该方案已成功部署在国内某领先双跨平台、明度制药、浙江兰溪纺织工业云平台等多个工业互联网平台安全的防护实践中，并在上海临港、广州白云、江苏无锡、浙江兰溪等多地落地区域安全保障子平台，为上百家工业企业提供安全托管服务。

典型部署案例：

（1） **国内大型工业互联网双跨平台安全防护案例**

图 5 工业互联网平台安全建设总体架构

针对上述平台架构，安恒信息整体采用 SaaS 化服务的设计思路，为该平台建设安全能力，围绕一中心、两体系、统一资源池建设，满足工业企业安全数据汇聚、多云异构兼容、服务分层解耦、新老应用并存等复杂安全需求，实现对云平台、大数据、应用、网络、边界、终端的全面安全赋能，通过一个运营平台实现整体安全运营，减轻运维工作量。

通过集中化的管理平台，实现云平台资源的集中化管理；通过建设集中的安全中心，实现安全能力的统一配置、运维，安全事件集中分析，展示全局安全态势，可实时对请求进行持续动态评估，构建整体安全防护能力。

（2）浙江兰溪纺织行业工业互联网平台安全防护案例

兰溪纺织行业中小企业和平台企业在进行工业互联网改造过程中，面临了一系列从上云前的业务安全到上云后的平台安全、终端接入、工艺数据、生产数据的安全性问题，从而导致企业对于上工业互联网平台积极性不足。安恒为其提供一体化安全防护解决方案，通过集中部署的工业互联网云安全中心，统一为兰溪工业互联网平台企业、纺织企业的公有云、私有云用户提供安全防护能力，实现安全集中建设、统一管理，穿管到从平台企业到联网企业。

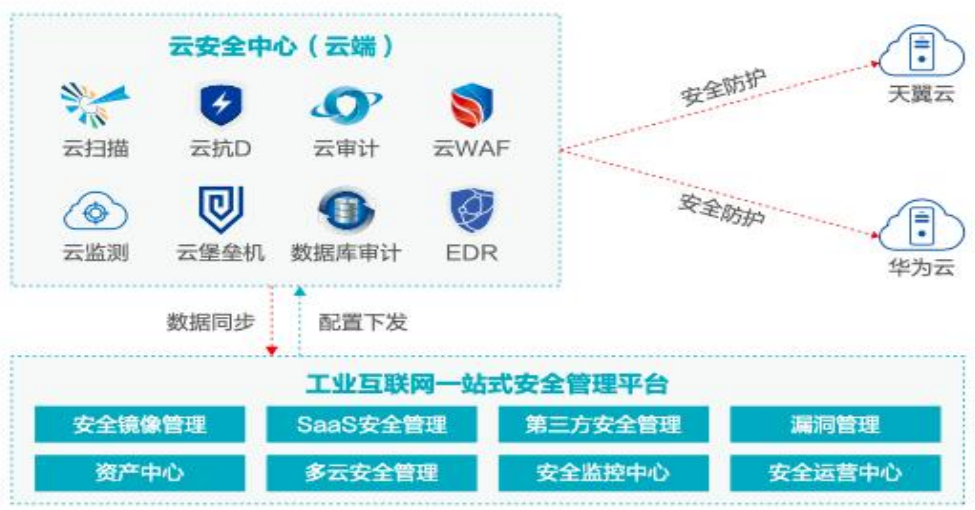

图 6 纺织行业工业互联网安全防护技术架构图

三、下一步实施计划

1. 提升工业互联网平台安全能力的标准化。本项目将从完善设备数据安全接入标准化、网络基础设施安全标准化、平台安全标准化、安全管理与运维标准化等方面，提升安全技术及产品质量，支撑工业互联网平台安全技术工程化开发及应用。

2. 通过项目实施，为国家推进工业互联网安全落地实施做出示范性意义及服务性表率，为验证国内互联制造服务云平台安全提供实际案例，为同行业类型企业的工业互联网平台综合安全防护体系建设树立典型应用案例。

未来该项目所形成的先进技术和模式将形成覆盖更多场景化的产品和技术，赋能更多行业，如智慧金融、智慧水务、智能制造等。

3. 推动工业互联网平台安全行业生态体系。目前平台已在上海临港区、浙江金华市、江苏无锡市等地实现规模化部署和服务，未来计划以平台化模式覆盖到更多的产业和多个工业互联网安全区域/行业子平台。以安全链接大中小企业以及上下游产业，在社会资源整合的力量下共同保障产业链、供应链稳定安全，高效助力企业步入数字化转型快车道。

四、项目创新点和实施效果

1. 项目先进性及创新点

（一）网络安全由“项目制”转向“SaaS 订阅制”的模式创新

在本项目中为某大型工业互联网平台提供了防御一体化、使用个性化、安全服务化、响应智能化的解决方案，网络安全赋能模式由传统的“项目制”模式向“SaaS 化订阅制”模式转变，实现安全能力的动态、弹性运维，满足平台和平台用户的多种个性化安全建设需求。按需购买、弹性订阅的特点，和高性价比的服务价格以及专业化的服务质量将形成安全服务新模式。

（二）基于机器学习的异常行为检测技术创新

本项目创新性地将机器学习应用进工业互联网的异常行为检测中。通过提取工业互联网系统中用户及网络设备之间访问行为的业务特征作为多维变量数据，对数据进行聚类分析并进行标记，再将标记后的数据再次分析并产生分类规则，经反复迭代，结合专家经验积累，形成针对工业互联网的异常行为检测技术，可以准确识别网络中的异常行为和恶意流量。

（三）基于隐患利用路径的威胁预警分析技术创新

本项目创新地将基于隐患利用路径的威胁预警分析技术在工业互联网平台安全领域进行了实践和落地。通过对工业互联网系统中各信息资产间存在的依赖关系，利用推理分析算法，通过被攻陷设备存在的隐患，推导出攻击者可能利用此隐患继续入侵到的其他信息资产并及时阻断。

（四）基于区块链的数据可信交换技术

工业互联网最重要的资产是数据，针对数据交换共享带来的数据泄露及数据主权问题，本项目创新性地使用基于区块链的数据可信交换技术，实现在可信执行环境中实现数据的可用不可见，数据使用可追溯的数据共享新模式。可信执行环境包含两部分，安全调试沙箱、安全计算沙箱。安全调试沙箱通过调试测试进行数据模型开发和数据模型验证。安全计算沙箱通过验证成功的数据模型运算数据集得到满足数据获益方需求的数据结果集。

2. 实施效果

通过本项目的应用与落地，工业互联网平台企业降低了在人力成本、物资资源、资金支出等方面的安全支出，完成了安全能力的全面建设，并随着安全运维、

安全运营工作的自动化、便捷化、智能化、实时化，降低了运维、运营复杂度，提升了运维、运营的工作效率，保障了工业互联网平台的稳定、高效运行。

（一）安全成效

本方案从设备、控制、应用、网络和数据五个维度，围绕企业在上云前、上云中、上云后的一系列安全隐患的防护，实现了对工业互联网的全方位安全覆盖，有效拦截了来自各个层面的网络威胁和攻击，降低了平台及平台上工业用户遭受网络攻击带来的安全风险，提升了平台系统等的可用性，保障了平台和平台上用户生产的正常运转，帮助建设安全可信的工业互联网平台，为国内工业互联网平台安全建设树立了标杆案例。

（二）经济效益

安恒信息的基于 MSS（安全托管服务）的工业互联网平台安全防护体系将安全运营能力 SaaS 化，有效降低了企业对于安全建设的成本，包括大量的人力成本和设备购置、维修、运行等硬件成本。例如人员的重复劳动、冗余的可复用数据、功能重叠的设备堆叠等重复投资，帮助企业摆脱机房建设、带宽租赁、网络建设等物资限制要求。SaaS 化的运营模式支持企业按需购买、弹性订阅，安全能力与服务随开随用，极大地降低了企业在安全建设上的人力、物资与资金投入。

（三）社会效益

一方面，本方案为设备自适应识别、区域边界防护、可信身份零信任服务、云平台态势感知、大数据分析、区块链等技术提供了落地场景和检验验证环境，有助于安全技术和产品的不断完善和优化，有助于工业互联网安全产业快速发展和成熟，创造可观的经济效益。

另一方面，本方案的落地切实有效地降低了工业互联网平台的安全风险，提升了该平台的整体安全防护能力，保障了系统持续稳定运行和数据隐私合规，有助于该解决方案在垂直领域、乃至跨行业跨领域的推广和复制，助力整个行业的安全建设，从而促进工业互联网产业安全、稳定、高质量地发展。

第三，平台保障联网企业安全上云，联网企业可以更放心地拥抱工业互联网，平台企业可以服务更多的联网企业，从而形成双赢的良性循环。