doi: 10.3969/j.issn.1672-6073.2022.06.010

云内云外融合网络安全纵深防御体系研究

史永飞
（厦门轨道建设发展集团有限公司，福建厦门 361010）

摘　要：基于城轨行业网络安全建设现状和国内外网络安全行业新技术应用调研情况，分析城轨云的网络安全风险，在遵循城轨协会各项技术规范和“平台统保、系统自保、边界防护、等保达标、安全确保”方针的基础上，研究城轨云内云外融合网络安全纵深防御体系建设方法，提出安全能力分步建设步骤和区分网域差异化安全能力构建理念，并探讨城轨云安全运维中心安全运营成熟度模型和各阶段目标，为后续城轨行业云平台安全规划建设提供指导。通过对软件定义安全、零信任、云工作负载、安全运维中心等创新技术进行对比分析，测试验证了相关技术在城轨云的创新应用场景，分析了创新技术所带来的技术效益。研究成果对于深化我国城轨云网络安全纵深防御体系具有一定的参考意义。

关键词：城轨云；网络安全；纵深防御；零信任；软件定义安全；主机安全；安全运维中心
中图分类号：U231　　**文献标志码：**A　　**文章编号：**1672-6073(2022)06-0059-05

Defense-in-depth System for Integrated Network Security Inside and Outside the Cloud

SHI Yongfei
(Xiamen Rail Transit Group Co., Ltd., Xiamen, Fujian 361010)

Abstract: Based on the current situation of network security construction in the urban rail industry and research on the application of new technologies in the network security industry at home and abroad, this study analyzes the network security risks of the urban rail cloud. Beginning with the 20-character policy of guaranteeing compliance and ensuring safety, we study a construction method for an urban rail cloud-integrated network security in-depth defense system, propose step-by-step construction steps of the security capabilities and concept of differentiated security capability construction in different network domains, and discuss the urban rail cloud. The security operation maturity model of the security operation and maintenance center and goals of each stage provide guidance for the subsequent security planning and construction of cloud platforms in the urban rail industry. A comparative analysis of innovative technologies such as software-defined security, zero trust, cloud workloads, and security operation and maintenance centers verifies the innovative application scenarios of related technologies in an urban rail cloud. The technologies introduced by the innovative technologies are analyzed. The results provide good reference significance for deepening the defense-in-depth system of urban rail cloud network security in China.
Keywords: urban rail transit cloud platform; network security; defense in depth; zero trust; software defined security; host security; security operation center

收稿日期：2022-08-08　修回日期：2022-09-13
作者简介：史永飞，男，硕士，工程师，长期从事信息化科研和管理等相关工作，10366888@qq.com
引用格式：史永飞. 云内云外融合网络安全纵深防御体系研究[J]. 都市快轨交通，2022，35(6)：59-63.
SHI Yongfei. Defense-in-depth system for integrated network security inside and outside the cloud[J]. Urban rapid rail transit, 2022, 35(6): 59-63.

随着大数据、云计算等技术在城市轨道交通行业的广泛应用，城轨云平台在呼和浩特、太原、深圳、南京等城市落地，武汉、西安等城市也完成了城轨云平台的规划和项目招标，调研已落地或完成招标城市的城轨云平台安全建设情况，并结合当前业内主流安全技术的发展[1]，笔者从技术与管理 2 个角度分析城轨云平台云内云外的网络安全风险。从技术角度来看，以太网、工控、LTE-M、WLAN 等网络传输协议又增加了 IoT、5G 等协议，意味着终端种类和数量都将爆发式接入，数据规模也从线性增长逐步变成指数型增长。传统认证方式+SSL VPN 设备无法满足内部管理网和外部服务网业务暴露面收敛需求；传统分散式安全设备难以应对未知威胁与新型攻击手段；全网安全威胁感知并不仅仅局限于以太网等网络协议的安全风险；传统的杀毒软件对重要业务系统容器化部署安全防护难以生效。从管理角度来看，面对网络安全这项老业务新领域，存在运维管理团队的安全技术人员缺乏，安全运营流程未完善，监管审计手段不足，内部人员意识薄弱等问题，因此难以形成标准或指标来量化管理。

本文通过对国家法律法规与行业规范的研究与分析，结合行业调研发现的技术与管理 2 方面的安全风险，提出安全能力分步建设步骤和区分网域差异化安全能力构建理念，明确边界防护要义和各网域安全架构设计，重点对软件定义安全、零信任、主机/终端安全、安全运维中心等创新技术应用进行深入论证，并在厦门地铁搭建测试环境，对安全资源池、安全态势感知平台、零信任平台等创新技术的核心产品进行应用测试成果验证，旨在通过对云内云外网络安全风险纵深防御的研究，为城轨云网络安全建设提供一定的经验借鉴，从而完善城市轨道交通网络安全体系建设。

1 城轨网络安全建设及运营思路

1.1 网络安全建设理念

针对目前城轨行业网络安全现状[2]，本文提出“智慧城轨网络安全防护体系”框架，如图 1 所示，左侧是智慧城轨技术框架[3]，右侧是包含“安全管理中心、物理环境防护、计算环境防护、区域边界防护、通信网络防护”的“一中心四防护”与“平台统保、系统自保、边界防护、等保达标、安全确保”方针[4]的相辅相成，打造网络安全和信息化一体两翼、驱动双轮，实现统一谋划、统一部署、统一推进、统一实施的建设思路，最终构建“体系化、常态化、实战化”的网络安全防护体系。

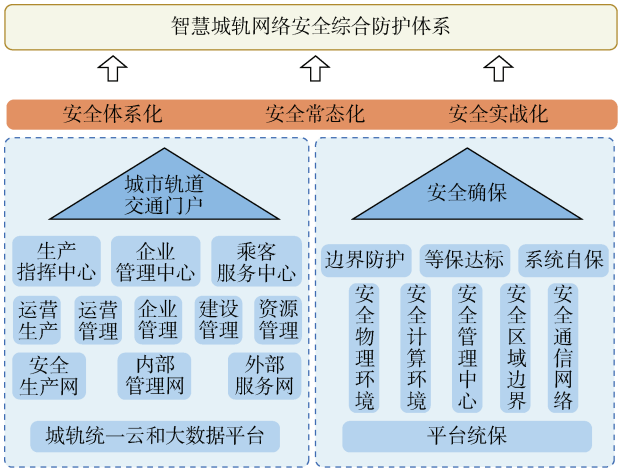

图 1 智慧城轨网络安全综合防护体系

Figure 1 Rail network integrated security protection system

1.1.1 安全能力分步建设思路

为了达到城轨云安全稳定运行的预期建设目标，支持城轨云每个阶段目标实现的安全能力规划和循序渐进的建设原则，本文提出“3 阶段”安全能力演进路径，具体如下。

第 1 阶段：夯实基础安全，合规零死角。构建以业务系统为核心的基础防御能力，覆盖边界安全防护、云计算平台安全、主要应用系统安全等方面，满足网络安全法要求的等级保护建设及行业监管标准规范要求。

第 2 阶段：构建动态防御，安全可视化。构建以安全大数据分析为核心的主动防御能力，配备专业安全运营服务和资源，融合软件定义安全、零信任、云工作负载平台等新技术，从而提升整体实战化安全能力水平，实现从“被动防御”向“主动防御”的进阶。

第 3 阶段：提升管控效果，安全持续发展。构建网络取证分析和威胁情报收集能力，能够发现未知威胁，结合自动化工具或手段开展安全监测、事件响应处置工作，能够 7×24 h 应对高级持续性威胁，以可量化的度量指标数据为基准，保障安全运营工作高效有序开展。

1.1.2 不同网域安全能力建设思路

根据《城市轨道交通云平台构建技术规范》[5]、《城市轨道交通云平台网络架构技术规范》[6]、《城市轨道交通云平台网络安全技术规范》[7]、《城市轨道交通线网运营指挥中心系统技术规范》[8]、《城市轨道交通大数据平台技术规范》[9]等标准规范，城轨云网络架构划分为运维管理网、安全生产网、内部管理网、外部服务网。不同网域的业务系统性质和安全等级各不相同，安全风险不同，应从边界到中心，从外到内，

构建纵深安全防护体系。其中，安全生产网以安全全域监测为主，采用双活数据中心架构；内部管理网以安全可信为主，从终端、用户、应用进行零信任设计；外部服务网以边界安全标准化为主，考虑主动防御，防外部攻击；运维管理网借助带外管理通道，安全信息同步，实现情报共享。

1.2 网络安全运营思路

目前城市轨道交通行业在网络安全运营方面的建设还处于初级阶段，网络安全运营的建设也缺乏评判依据，需要建立成熟度模型来判断其发展程度。

因此，在前期研究及行业调研基础上提出了网络安全运营的成熟度模型。网络安全运维中心的成熟度分为 5 个阶段。

1) 初始状态：仅布局基础安全设备；

2) 基础运行：满足安全合规化建设与维护；

3) 运行可控：以安全能力与标准化流程构建为主；

4) 体系运营：实现安全运营体系化建设及安全价值的输出；

5) 深度运营：具备完善的安全运营能力及技术与管理探索。

城轨企业网络安全运维中心的成熟度模型的每一个维度、因素和方面都沿着成熟度的 5 个阶段进行构建，用来帮助城轨企业确定目前的安全运维中心的能力水平。网络安全运维中心的成熟度模型能够帮助城轨企业快速找到安全运营中的短板并制定有针对性的策略，加速将安全运营融入企业文化中，提升常态化、实战化安全能力。

城轨企业的安全运维中心应该具备不同的阶段目标，做到有的放矢。因此，要设定城轨云安全运维中心每个阶段成熟度的目标，具体如表 1 所示。

表 1 安全运维中心运营成熟度目标

Table 1 Operational maturity goals of security operation and maintenance center

级别	状态	运营成熟度目标
1 级	初始状态	处在基础设施建设阶段，安全建设以基础预防为主，资产不清晰、缺少漏洞管理机制，对整体安全威胁不可见，没有事件响应处置流程。
2 级	基础运行	安全建设以合规为主，有资产管理动作及漏洞管理认知，对安全威胁有一定可见性，但不具备与威胁事件深入分析的能力，没有建立成熟的事件响应流程。
3 级	运行可控	安全运营团队各岗位职责明确，资产管理及漏洞管理已形成常态化流程与机制，具备威胁监测、分析及时间处置能力，对整体安全威胁态势可见，有成熟的时间响应流程，具备初步的量化管理。
4 级	体系运营	具有安全事件响应中心或安全运维中心等安全运营常态组织，运营团队各岗位之间紧密配合，资产、漏洞等基础工作扎实有效，能够高效地开展监测、响应、处置、调查取证分析工作，能够积极主动挖掘威胁情报，能够应对高级持续性威胁。
5 级	深度运营	除可自主成熟开展各项安全运营工作外，具备网络取证分析和威胁情报收集能力，能够发现未知威胁，使用自动化工具或手段开展安全监测、事件响应处置工作，能够 7×24 h 应对高级持续性威胁。

2 网络安全纵深防御体系应用技术

2.1 软件定义安全技术

目前软件定义安全的技术路线有 3 种，包括硬件一虚多、网络虚拟化、安全资源池，3 种软件定义安全技术路线对比见表 2。

表 2 软件定义安全技术路线对比表

Table 2 Comparison of software-defined security technology routes

特点	硬件一虚多	网络虚拟化	安全资源池
功能	安全功能少，只能实现传统的防火墙、VPN 等	功能丰富，融合主流安全功能，包括负载均衡、日志审计、运维审计等	功能丰富，融合主流安全功能，包括负载均衡、日志审计、运维审计等
性能	单台设备性能较高，开启虚拟化后性能骤降	依赖 X86 服务器的 CPU、内存配置	依赖 X86 服务器的 CPU、内存配置
可靠性	无	通过网络选路实现，可靠性一般	支持副本，HA 机制，可靠性高
灵活性	差	高	高
管理性	无可视化界面	统一纳管，管理简便	统一纳管，管理简便
可扩展性	对网络改动较大	依赖于云计算硬件平台资源	南北向、东西向均可扩展
稳定性	依赖硬件设备，稳定性强	与硬件、软件兼容性有关，稳定性一般	与虚拟化环境有关，稳定性强

通过对比 3 种技术路线的功能特点及适用场景，安全资源池具有高开放性、高可靠性与丰富的功能等特点，更适合作为城轨行业云平台安全防护措施。此外，安全资源池的部署方式与等级保护所需的安全组件开通方式更加灵活，本文重点对安全资源池与云平台的对接进行研究，包括传统 API 接口对接(云管平台与安全资源池独立管理)与云服务注册方式(云管平台统一管理)2 种方式。其中云服务注册方式更加符合“一云统管”理念。

对解耦合的安全资源池进行测试，由安全厂商提

供安全资源池设备，与云平台进行对接测试，包括安全资源池的可靠性、可维护性、可扩展性、与云管平台对接等功能，验证了安全资源池确实更适合作为城轨行业云平台安全防护措施。同时对安全资源池与云平台对接的 2 种方式进行验证：1)通过传统 API 接口的方式，实现云平台与安全资源池的信息同步功能及基于业务申请安全组件的功能；2)通过云服务注册方式进行安全资源池与云平台对接。对比发现云服务注册方式对安全资源池架构调整较大。传统 API 接口对接方式则对安全资源池架构改动较小，绝大部分安全厂商均可完成适配，是业界主流的对接方式。城轨云应综合考虑改造周期、定制成本、运维效率、对接效果、功能丰富性等因素，进行安全资源池的建设。

2.2 主机/终端安全技术

终端安全的核心能力需求主要包括病毒防护、漏洞管理、入侵防护 3 个部分。本文研究了传统杀毒、终端安全检测响应、云安全工作负载 3 种技术路线的特点，见表 3。

表 3 主机/终端安全技术路线对比表

Table 3 Comparison of endpoint security technology routes

功能	传统杀毒	端点检测与防护	云工作负载平台
概况	主要针对已知病毒：提取已知病毒特征，并将其特征更新至病毒库，用户通过升级杀毒软件才能应对	传统杀毒能力+未知病毒查杀+入侵行为检测+运维管理能力(偏重于杀毒)	杀毒能力+更强的入侵行为检测+更强的脆弱性管理能力(偏重于脆弱性管理、入侵行为检测)+容器安全
防护细粒度	操作系统级	操作系统级	应用级，容器级(支持容器 agent)
暴露面管理	不支持	支持	支持
入侵检测	不支持	支持	支持
病毒防护	仅支持已知病毒防护	支持已知病毒+未知病毒防护	支持已知病毒+未知病毒防护
无文件攻击防护	不支持	支持	支持
风险评估	不支持	补丁管理(操作系统级补丁)、基线核查	补丁管理(应用级补丁、容器镜像漏洞管理)、基线核查
攻击溯源分析	不支持	支持访问流量可视，便于攻击溯源分析	支持容器访问可视化展示

其中云工作负载平台技术因其轻量化、入侵防御能力强的特点，解决了传统杀毒处置方式落后、无法有效抵御新型攻击与病毒、安全边界模糊等问题，能够更好地满足城轨云主机安全建设需求，并符合容器化趋势。

通过进行云工作负载平台对业务系统安全防护效果的相关测试，本文认为云工作负载平台在容器安全防护、漏洞补丁管理、自适应微隔离能力更为突出。云工作负载平台可以重点解决有效防御高级持续性威胁的问题，实现城轨云工作负载的防护加固，避免渗透攻击；构建工作负载的微隔离边界，避免横向威胁等。同时可对虚拟主机、宿主操作系统、容器进行安全防护。因此，云工作负载平台更加符合构建城轨云工作负载的安全防护体系，满足终端安全建设的实战化安全需求。

2.3 零信任技术研究与应用

业界基于零信任主要通过 3 类技术的结合，在一定程度上满足零信任的要求规范，这 3 类技术分别为统一身份认证、软件定义边界和微隔离。通过实现用户到业务的网络分段以及工作负载间分段的结合达到零信任的效果。

通过前期调研城轨行业业务场景分析，零信任架构在城轨行业的场景应用主要分为 3 方面。

1) 通过统一身份认证系统建设城轨内部管理网统一数字化身份认证和权限管理能力，对人员、设备、应用、服务赋予数字身份信息，对身份账号密码进行全生命周期管理，对访问权限进行统一配置管理[10]。

2) 通过零信任客户端、零信任网关、零信任控制中心组成软件定义边界零信任访问体系，对移动办公、远程运维场景进行管控。零信任客户端负责发起访问请求，并且具备终端环境感知能力，通过安全基线判断终端安全可信。零信任网关负责鉴权验证访问请求，隐藏发布端口，同时具备行为审计安全能力。零信任控制中心负责策略配置与下发和威胁识别的能力，具备分析用户访问行为、终端环境评分等能力，同时可对接统一身份认证系统和外部安全组件同步安全风险，动态判断实时安全性，及时调整访问策略[11]。

3) 通过架设 API 网关，实现业务应用接口的安全管控，将业务应用服务 API 接口、数据服务 API 接口进行代理，实现访问流量加密、权限控制、内容验证等效果，收缩接口暴露面，加强业务接口访问的安全性。

本文对零信任架构在城轨行业的应用场景进行分析，并对相关功能进行测试验证，包括主机微隔离、远程安全访问、身份鉴别与应用代理等方面，充分证明通

过统一身份认证技术可解决运维管理网和内部管理网统一身份认证的问题；通过软件定义边界技术可解决可信终端的判定以及可信终端接入后的权限问题；通过微隔离技术可实现运维管理网和内部管理网云工作负载之间的精细化访问控制及异常访问所提供的告警功能。

2.4 安全运维中心

实战化的安全运营体系是保障城轨业务安全稳定运行的基础，通过信息安全运营活动将静态的信息安全产品变为动态的信息安全防护体系并持续改进。目前城市轨道交通行业在网络安全运营方面的建设还处于基础阶段，安全防护能力较为薄弱，缺少站在宏观角度上常态化、实战化的安全运营能力，需要通过“人+平台+流程制度”建设城轨云平台安全运维中心，结合城轨云业务实际场景全面提高厦门城轨企业安全运营能力至深度运营阶段。

根据全面收集、智能关联、快速处置、直观展现的原则建立城轨企业态势感知与安全运营平台，该平台为城轨企业安全运营工作的信息汇聚中心、安全分析中心、安全指挥中心。平台实时采集各类检测信息、告警信息、审计信息等，结合威胁情报，对安全数据进行集中分析，识别安全威胁，实现安全风险的智能感知和动态研判[11]。同时建立事件处置流程，结合协同处置机制，实现对安全事件的快速处置。平台能够直观展现并提供完整、易用、高效的人机分析界面供安全运营人员进行快速地分析判断，提高运营效率。

对于云平台缺少虚拟私有云内部东西向流量检测手段的问题，通过引入运维技术平台及云内软探针技术，实现云内东西向流量检测[12]。按照等级保护对工控网络的安全要求，通过线网安全态势感知平台对接工控域安全管理平台，对接线路的安全管理平台和安全设备，实现全域安全统一监测。

通过预先针对城轨云平台安全运维中心技术平台进行功能测试验证，包括资产及脆弱性发现、数据归一采集、安全设备联动等，其中重点进行了安全运维中心与安全设备的联动功能验证，解决了在城轨云全域安全监测及协同联动处置等方面的难题，并支持联动安全设备进行攻击溯源，回溯完整攻击过程，这对于城轨企业实现基础自动化告警处置提供了借鉴，也为未来实现安全编排自动化与响应技术(security orchestration automation and response，SOAR)做好铺垫。

最终平台结合城轨企业安全运维人员及流程制度，形成常态化安全运维中心，提高城轨企业安全运维中心成熟度，为业务安全有序运转提供有力保障，为城轨行业安全运维中心成熟度建设提供实践参考。

3 结语

通过实测和分析网络安全技术在城轨云平台安全生产网、内部管理网、外部服务网等多个场景的创新应用，提出了城轨云网络安全建设的新思路，从整体上提升了城轨云平台网络空间安全防护水平和科学应对网络安全威胁的能力，构建出能够实时发现问题、应对风险、可持续发展的实战化网络安全保障体系，旨在为我国城轨云网络安全纵深防御体系建设提供参考和依据。

参考文献

[1] 中国城市轨道交通协会. 中国城市轨道交通协会印发《中国城市轨道交通智慧城轨发展纲要》[J]. 现代城市轨道交通, 2020(3): 105.

[2] 智慧城市轨道交通信息技术架构及网络安全规范 第 1 部分：总体需求: T/CAMET 11001.1—2019[S]. 北京：中国铁道出版社有限公司, 2019.

[3] 智慧城市轨道交通信息技术架构及网络安全规范 第 2 部分：技术架构: T/CAMET 11001.2—2019[S]. 北京：中国铁道出版社有限公司, 2019.

[4] 智慧城市轨道交通信息技术架构及网络安全规范 第 3 部分：网络安全: T/CAMET 11001.3—2019[S]. 北京：中国铁道出版社有限公司, 2019.

[5] 城市轨道交通云平台构建技术规范: T/CAMET 11002—2020[S]. 北京：中国铁道出版社有限公司, 2020.

[6] 城市轨道交通云平台网络架构技术规范：T/CAMET 11004—2020[S]. 北京：中国铁道出版社有限公司, 2020.

[7] 城市轨道交通云平台网络安全技术规范：T/CAMET 11005—2020[S]. 北京：中国铁道出版社有限公司, 2020.

[8] 城市轨道交通线网运营指挥中心系统技术规范: T/CAMET 11006—2020[S]. 北京：中国铁道出版社有限公司, 2020.

[9] 城市轨道交通大数据平台技术规范: T/CAMET 11003—2020[S]. 北京：中国铁道出版社有限公司, 2020.

[10] 李崇智. 基于零信任架构的统一身份认证平台应用研究[J]. 信息安全研究, 2021, 7(12): 1127-1134.
LI Chongzhi. Application research of unified identity authentication platform based on zero trust architecture[J]. Journal of information security research, 2021, 7(12): 1127-1134.

[11] 魏小强. 基于零信任的远程办公系统安全模型研究与实现[J]. 信息安全研究, 2020, 6(4): 289-295.
WEI Xiaoqiang. Research and implementation of security model of telecommuting system based on zero trust[J]. Journal of information security research, 2020, 6(4): 289-295.

[12] 李绪国, 曹瑜, 王建兴, 等. IT 与 OT 网络安全态势感知平台联合开发技术与实践[J]. 通信技术, 2021, 54(1): 209-214.
LI Xuguo, CAO Yu, WANG Jianxing, et al. Joint development technology and practice of IT & OT network security situation awareness platform[J]. Communications technology, 2021, 54(1): 209-214.

（编辑：王艳菊）