大型企业SASE解决方案及应用实践

SASE Technology Solution and Implementation Practice for Large Enterprise

王茜/WANG Qian，陈晨/CHEN Chen，井俊丰/JING Junfeng，季家震/JI Jiazhen

（奇安信科技集团股份有限公司，中国 北京 100032）
(QI-ANXIN Technology Group Inc. , Beijing 100032, China)

DOI：10.12142/ZTETJ.202301009
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20230223.1047.002.html
网络出版日期：2023-02-23
收稿日期：2022-11-25

摘要：针对大型企业的数字化转型和提升安全防护水平的需求，基于安全访问服务边缘（SASE）架构设计了企业一体化安全运营系统Q-SASE及其技术实现方案。Q-SASE不仅可以对分支机构众多的企业提供统一安全防护水平、统一安全访问策略和统一安全运营能力，还可以在后疫情时代支持移动办公场景的终端身份管理和可信安全接入。在大型企业中的落地实践验证了Q-SASE技术方案的可行性和有效性。

关键词：SASE；云安全资源池；零信任；网络安全态势感知；安全运营中心

Abstract: In response to the digital transformation and improvement of the security protection level of large enterprises, based on the secure access service edge (SASE) architecture, an enterprise integrated security operation system Q-SASE and its technical scheme are designed, which can not only provide a unified security protection level, unified security access policies, and unified security operations for enterprises with many branches , but also support identity management and secure access of user equipment in mobile office scenarios in the post-epidemic era. The feasibility and effectiveness of this Q-SASE technical solution have been verified through the implementation practice in large enterprises.

Keywords: SASE; cloud security resource pool; zero trust; network security situational awareness; security operations center

近年来，企业业务系统向云化迁移，信息数据日趋集中化。各种信息化系统趋于集中式建设和分布式服务。新型基础设施如新型广域网、移动互联网、混合云、泛终端、大数据平台的出现，也让信息化系统的建设和运维模式发生变化。同时，网络安全形势日趋复杂，网络攻击手段更为多样。数据泄露、勒索软件、高级可持续威胁（APT）攻击等安全事件频发。相应地，针对这些安全威胁的实战化、体系化、常态化要求也变得越来越高。信息技术（IT）、网络、安全需要统筹管理。同步规划、同步建设、同步运营已成为企业数字化转型的必然要求。

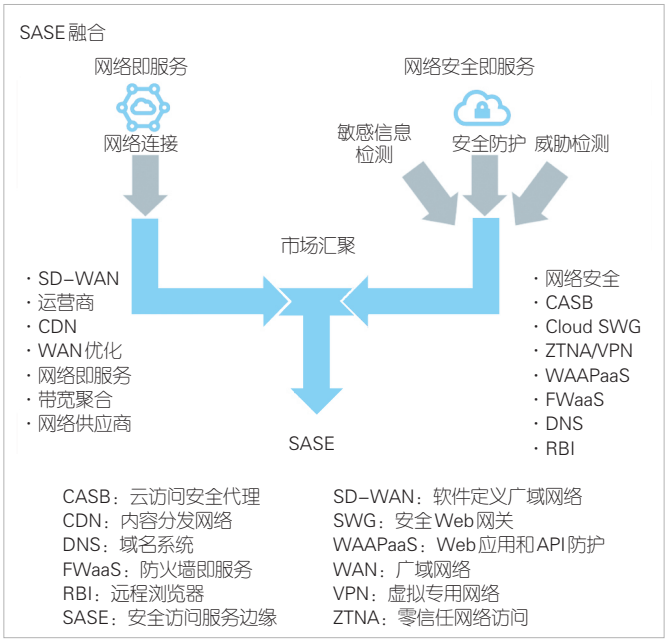
但是，中国的企业信息化网络依然面临着防护不全、投入不足、能力不够、效率不高等问题。尤其是那些具有众多分支机构的大型企业，其分支机构分布广、防护范围广、防护点多，且各分支机构的安全防护能力参差不齐，难以实现统一管理和安全防护。另外，全球疫情的蔓延使办公环境从局域网延伸到居家办公（SOHO）场景。各类自带设备（BYOD）终端已成为企业办公环境的接入边界。漏洞、后门、僵尸木马等针对终端设备的安全威胁日益严重。黑客更容易入侵各类智能设备，渗透企业网络和重要的业务系统，窃取用户数据或者企业经营数据。这将给企业带来直接和间接的经济损失。

基于Gartner提出的安全访问服务边缘（SASE）架构，我们设计了针对大型企业的一体化安全运营系统Q-SASE，通过“软件定义安全”“软件定义网络”“零信任动态评估”等技术实现了整体解决方案，并通过在大型企业的落地实践，对Q-SASE的一体化安全运营的可行性和有效性进行了验证。本研究可作为行业推广的经验参考。

1 基于SASE架构的解决方案

1.1 SASE架构的由来

2019年Gartner在《未来的安全在云端》中提出了SASE的概念。Gartner官方对SASE的定义如下：SASE通过将网络和网络安全的功能融合为统一服务的模式，为企业客户提供一个新的网络安全架构，如图1所示。SASE能够使分支机构人员和移动办公用户高效、安全地就近接入安全节点（部署在云端或者数据中心的PoP点），以访问互联网应用、公



▲图1 SASE技术概念图

有云软件即服务（SaaS）、公司内部应用等。

根据Gartner的定义，SASE是一种基于实体的身份、实时上下文、企业安全/合规策略，以及在整个会话中持续评估风险/信任的服务。实体的身份可与人员、人员组（分支机构）、设备、应用、服务、物联网系统或边缘计算场地相关联。SASE架构将使安全运营以一致和集成的方式提供一组丰富的安全网络服务，从而支持企业数字化转型和业务向云计算的迁移，并满足员工移动办公的需求。

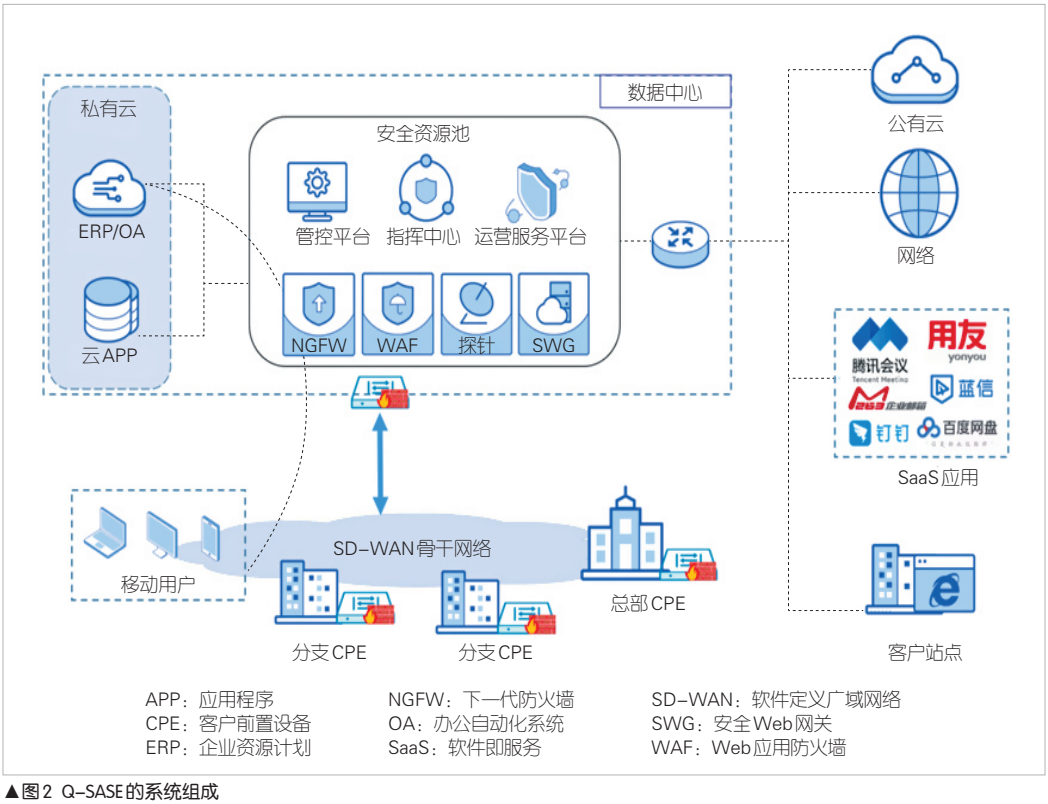
1.2 Q-SASE解决方案

基于SASE架构和零信任理念，Q-SASE解决方案采用“软件定义广域网络（SD-WAN）+软件定义安全+零信任动态信任”的技术路线，实现了针对大型企业的分支机构和移动办公场景下访问互联网、公有云、私有云内部应用的整体安全防护。其中，SD-WAN技术对分支机构的各类访问流量进行组网编排和引流，软件定义安全的云安全资源池对多种访问流量进行安全防护，零信任技术对接入的用户终端进行身份认证和动态访问控制。因此，Q-SASE能够实现组网和安全功能相融合的整体解决方案。

Q-SASE解决方案包括一套安全运营管理服务平台，以及为企业客户建设的云安全资源池，通过在分支机构部署SD-WAN安全网关，以及移动办公终端安装零信任客户端，将访问互联网、内网业务系统的流量引流到安全资源池进行安全防护和安全威胁检测分析，并在威胁检测分析的基础上，提供“安全运行闭环管理并持续监测响应为核心”的安全运营，如图2所示。

1）Q-SASE的安全运营管理服务平台。该平台能够对整个SASE架构中的系统模块进行持续运行监测，以保障整个系统的持续稳定运行。此外，该平台还可对运营人员的权限和工单进行管理，实现对安全告警日志和安全事件的持续跟踪与管理，并基于企业需求针对安全资源池和安全网关中的组网策略和安全策略进行持续优化。

2）Q-SASE的安全资源池。安全资源池采用虚拟化镜像的方式来部署不同的安全组件。安全资源池的安全组件按需配置。安全组件的创建、初始化、激活等操作都由安全资源池来支撑系统自动完成。在不同分支机构的SD-WAN安



▲图2 Q-SASE的系统组成

全网关接入资源池前，安全资源池将支撑系统，使系统按照不同租户角色申请来部署安装相应的安全组件。安全访问服务的云安全资源池采用虚拟化方式部署，可基于接入的分支机构数量和互联网流量规模实现弹性扩容。根据不同企业的需求，安全资源池可部署丰富的安全组件，包括虚拟化防火墙安全组件、上网行为审计安全组件、零信任接入安全组件、虚拟化Web应用防护（WAF）安全组件、日志审计安全组件、态势感知云探针安全组件等。

3）SD-WAN组网及引流。采用SD-WAN技术，安全网关与安全资源池之间可实现快速灵活组网，并支持将分支机构访问互联网应用和内网应用的流量引流到安全资源池以进行安全防护和安全运营。安全网关设备支持零配置开局部署，并支持自动注册及从运营管理平台获取初始化网络配置和安全策略配置，还可通过预配置向导、批量脚本导入、邮件零配置上线（ZTP）、无线网络ZTP等多种方式，实现分钟级零配置上线。安全网关还支持灵活接入能力，可以支持专线接入、互联网以及4G/5G移动网接入。

4）零信任客户端接入。基于零信任客户端对可信访问控制台和可信应用代理的访问，从身份风险、终端风险、网络风险、权限和数据风险5个维度，全面构建从终端到应用访问的端到端安全防护信任评估能力。便捷的运维管理能力和动态访问控制机制，可确保在业务访问的各个阶段都能拥有较好的零信任防护效果。零信任可信客户端对接入终端的用户进行身份认证，支持账号的统一管理与单点登录，拥有权限管理与多因子认证等安全能力；支持对终端的应用环境进行实时监测，即只有通过终端环境信任评估的才能接入政企客户内部网络，例如是否安装杀毒软件、是否升级到最新版本和最新病毒库；基于终端的身份管理，可以依托企业的4A（包括认证、账号、授权、审计）、身份识别与访问管理（IAM）、Windows服务器的活动目录（AD）、轻量目录访问协议（LDAP）、公钥基础设施（PKI）等基础设施，也可以基于企业自建的身份认证中心和应用访问会话，对所有访问请求建立动态访问控制策略。

2 Q-SASE的关键技术实现

基于SASE的创新型架构和内生安全框架，Q-SASE方案采用“软件定义网络”“软件定义安全”和“零信任动态评估”3种技术，不仅实现了SD-WAN技术的灵活组网和引流，还实现了云安全资源池的按需交付和分布式部署，以及零信任的身份管理和信任评估动态控制，并基于实时威胁检测实现了安全风险分析与协同处置。

2.1 软件定义网络技术方案

Q-SASE采用SD-WAN的技术路线，而SD-WAN是基于软件定义网络（SDN）的技术体系发展而来的。Q-SASE实现了SDN管控平台与安全网关的协同工作机制。

SDN采用与传统网络截然不同的控制架构，将网络控制平面和转发平面分离，采用集中控制替代原有分布式控制，并通过开放和可编程接口实现软件定义。SDN技术架构如图3所示。

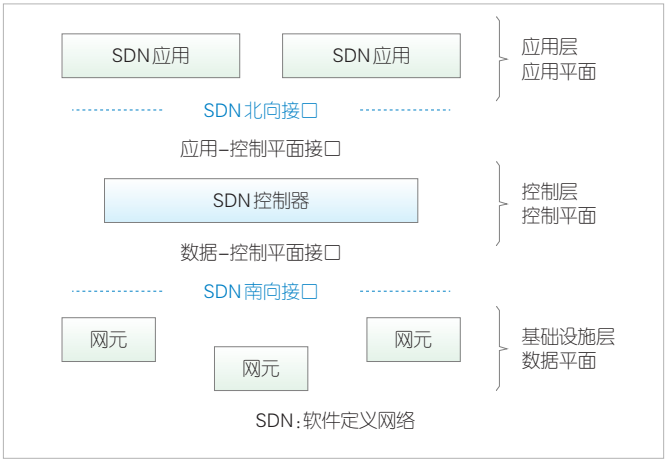
从网络架构层次上看，SDN典型的网络架构包括转发层（基础设施层）、控制层和应用层。该新技术会对组网技术产生以下积极的影响：

1）降低设备复杂度。转发和控制的分离，使得网络设备转发平面的能力要求趋于简化和统一，硬件组件趋于通用化而且便于不同厂商设备的互通。这些都有利于降低设备的复杂度和硬件成本。

2）提高网络利用率。集中的控制平面可以实现海量网络设备的集中管理，使得网络运维人员能够基于完整的网络全局视图实施网络规划，优化网络资源，提高网络利用率，降低运维成本。

3）加速网络创新。一方面，SDN通过控制平面可以便捷地为网络设备制定各种策略，提升网络灵活性；另一方面，SDN提供开放的北向接口，允许上层应用直接访问所需的网络资源和服务，使得网络可以差异化地满足上层应用需求，提供更灵活的网络服务，加速网络创新。

SD-WAN是将SDN技术应用到广域网场景中的一种实践方案。这种方案用于连接广阔地理范围的企业网络、数据中心、互联网应用及云服务，旨在帮助企业降低广域网的开支，提高网络连接灵活性。SD-WAN作为SDN技术体系中的一种可落地的门类，为企业带来了低成本、高可用带宽的



▲图3 软件定义网络技术方案

组网方式。

2.2 软件定义安全技术方案

“软件定义”作为一种理念，可以从网络领域沿用到安全领域。云安全资源池作为Q-SASE解决方案实现的重要载体，其背后的技术支撑正是软件定义安全（SDS）。云安全资源池也是软件定义安全技术的核心应用方向之一。

云安全资源池技术方案的目标在于“随需而变”，而这正符合软件定义安全敏捷、高效、开放的特点。云安全资源池需要运行在云计算环境中，不仅要解决传统安全能力落地的问题，还要能够充分发挥云计算基础设施的功能与优势，实现快速交付、分布式部署、多云（含信创）环境支持、服务链编排等。

在软件定义安全的技术实现中，安全管理控制是重中之重。这是因为安全管理控制承担了所有安全能力的服务抽象、服务编排及调度、策略管理、策略交付等安全核心功能。此外，安全管理控制还需要实现与云平台的深度集成，基于应用程序编程接口（API）获取云上租户资产的关键信息，以便安全管理员部署和管理所需的安全资源。

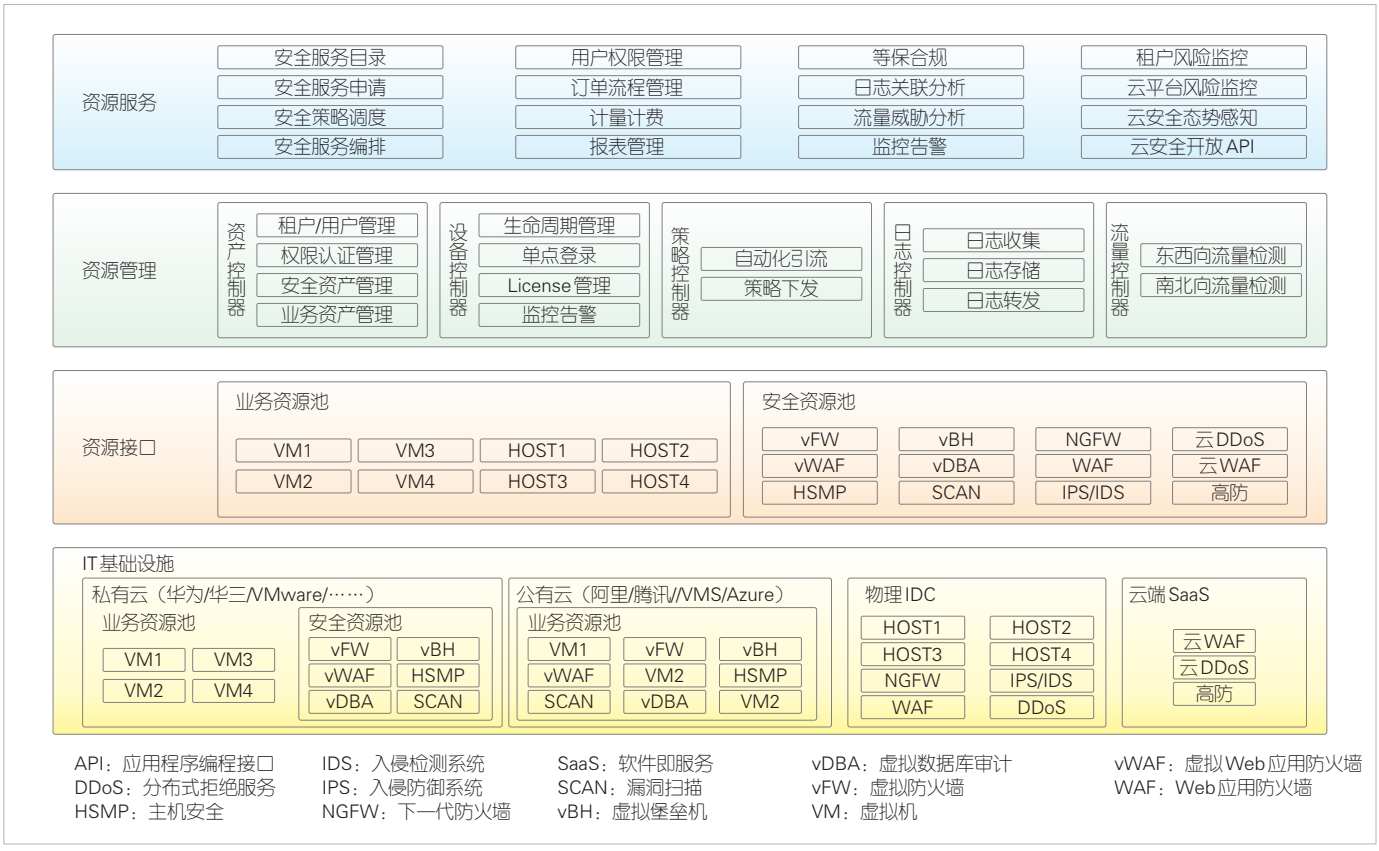
Q-SASE中的云安全资源池，技术方案架构如图4所示。

此外，云安全资源池南向对安全能力完全开放，可通过定义安全组件的统一接入规范来支持各类安全能力，包括第三方安全能力的接入；北向通过开放API支持平台的能力和用户的业务系统深度融合；西向通过定义标准的服务链编排接口支持各种引流设备，包括传统的交换机引流和SDN控制器引流；东向则通过定义标准的云平台对接技术规范来统一支持各种私有云、公有云等云平台的对接，实现云平台租户、资产、用户的同步和管理。

2.3 零信任身份管理及信任评估技术方案

零信任技术方案关注业务保护面的构建，通过业务保护面实现对资源的保护。在零信任方案中，应用、服务、接口、数据都可以作为业务资源。该方案通过构建保护面实现对暴露面的收缩，要求所有业务默认隐藏，并根据授权结果进行最低程度的开放。所有的业务访问请求都应该进行全流量加密和强制授权。业务安全访问相关机制需要尽可能工作在应用协议层。

基于身份而非网络位置来构建访问控制体系，首先需要为接入网络的人和设备赋予数字身份，将身份化的人、设备和应用进行运行时组合构建访问主体，并为访问主体设定其



▲图4 软件定义安全技术方案

所需的最小权限，以进行全面数字化管理。其中，访问主体由用户、设备和应用组合而成。系统会在身份管理的基础上进行持续信任评估，并通过信任评估模型和算法，实现基于身份的信任评估能力，同时需要对访问的上下文环境进行风险判定，对访问请求进行异常行为识别，并对信任评估结果进行调整。在身份信任的基础上，系统还需要评估主体信任。主体信任是对身份信任在当前访问上下文中的动态调整，和认证强度、风险状态和环境因素等相关。身份信任相对稳定，而主体信任和网络代理一样，具有短时性特征，是一种动态信任。

基于主体的信任等级进行动态访问控制是零信任技术方案的本质所在。动态访问控制采用基于角色授权（RBAC）和基于属性授权（ABAC）的组合授权模式。这样便于系统实施灵活的动态访问控制。基于安全基线叠加信任等级可实现分级的业务访问。同时，当访问上下文和环境存在风险时，系统需要对访问权限进行实时干预，并评估是否需要对访问主体的信任进行降级。

2.4 安全威胁分析及协同处置技术方案

在日常的安全运营工作中，真正的威胁往往会被淹没在大量的未确认安全事件中，如低危的防火墙、IDS和WAF告警等。然而，这些告警的分析确认和处置往往会成为令人头疼的问题。传统的安全检测能力主要依托特征库匹配的检测机制。虽然这样能够有效地检测并拦截普通的低级威胁，但也会产生大量的冗余和误报告警。如果不对安全策略和检测机制进行优化，安全运营人员就无法在发生威胁的第一时间判断出哪些威胁会造成严重影响，哪些威胁需要优先处置。

基于大数据架构设计的流式关联分析引擎，能够实时关联多维度数据，结合云端的威胁情报样本，可以针对使用不同日志数据（如入侵防御日志、上网行为日志等）检测内部主机连接攻击者远程命令和控制服务器，进而发现失陷主机的安全威胁，防止由失陷带来的数据泄密、系统破坏等关键风险。基于云安全资源池的本地威胁情报，配合云端威胁情报分析平台进行进一步的分析，了解安全威胁的背景信息，以及攻击者的相关网络资源和历史攻击行为，并进行深入追踪，通过多数据关联分析和威胁溯源，实时提供攻击者上下文信息，提升威胁分析、溯源和协同处置的效率。

3 Q-SASE的应用实践

基于中国电子信息产业集团有限公司（简称中国电子）的一体化安全运营需求，结合企业数字化转型的业务发展目标，我们构建了包括Q-SASE运营管理服务平台，云安全资源池的安全防护组件、零信任组件，以及SD-WAN安全网关和零信任客户端在内的Q-SASE一体化安全运营系统，为中国电子26家二级企业的240家分支机构和超过12万员工的公有云、行业云终端访问业务，提供覆盖云网端的安全防护和安全运营能力。

在中国电子的3类企业信息系统访问场景中，Q-SASE重点实现以下系统建设和安全防护：

1）采用新型SD-WAN技术，建设覆盖全部二三级企业的广域网，并将各分支机构的互联网访问流量进行汇聚，统一实现互联网出口集中管理和安全防护；

2）根据数字中国电子自身业务发展和未来业务系统集中上云的规划，在北京、武汉、深圳等云数据中心部署分布式的安全资源池，具备针对统一互联网出口流量和内部业务系统访问流量的安全防护能力和零信任安全访问能力，对集团总部、所属二三级企业以及新建云数据中心之间的网络通信安全、公有云和行业云业务系统安全、办公访问安全进行有效保障；

3）依托云安全资源池的安全防护组件和零信任组件的能力，以及态势感知的威胁发现能力，通过专业的安全运行团队进行持续巡检监测、故障发现、处置保障、策略优化等安全运行闭环，周期性安全评估安全防护系统平台自身的安全性，提升网络安全攻防演练期间的统一安全防护效果；

4）结合数字中国电子的实际组织架构现状，建立全集团统一安全运营服务中心，将原有纯建设的防护交付模式，演进为以安全服务保安全效果的服务交付模式，从“集团业务全应用场景”的角度出发，全面考虑“集团网络安全职能落地”“各单位网络安全职责落地”所需的工作内容，贴合设计、服务保障。

中国电子是以网络安全和信息化为主业的国有信息技术（IT）企业，也是兼具计算机中央处理器（CPU）和操作系统关键核心技术的中国企业。Q-SASE提供的安全防护和安全运营不仅能够覆盖公共通信和信息服务业，计算机、通信和其他电子设备制造业，还覆盖专用设备制造业、商务服务业、批发业等多个国民经济行业。在基于Q-SASE方案进行一体化安全运营过程中，系统累计发布42期安全周报，下发110份安全事件通告，累计处理74.3万条告警（其中有危急告警8.4万条、高危告警22.7万条）。前10位的攻击类型和所占比例分别为：SQL注入占23.11%，信息泄露占11.82%，代码执行占9.50%，命令执行占4.67%，弱口令占4.04%，暴力猜解占4.03%，跨站脚本攻击占2.59%，网络扫描占2.39%，配置不当/错误占2.29%，非授权访问占1.34%。Q-SASE通过及时分析监测发现威胁及安全事件，同步开展

响应和处置工作，并通过策略编排及时阻断病毒文件、间谍软件横向传播等风险，形成预警及处置报告。Q-SASE方案在中国电子集团总部南迁、重大活动网络安全保障、挖矿行为自查自纠、国家级实战攻防演练等活动中，均取得明显成效。

4 总结和展望

Q-SASE的整体解决方案，将原有分散在各分支机构的网络安全设备集中到云安全资源池，以进行统一建设，实现分支机构的互联网和内网访问流量的收口和统一的安全防护与安全运营。Q-SASE的应用实践表明，Q-SASE方案可以系统性、工程化地实现安全防护和安全运营能力的集中部署、集中运行和统一运营，使大型企业的分支机构快速具备网络安全能力，在疫情常态化后的困境中，让灵活、安全的办公和安全上云的访问成为可能，为企业数字化转型保驾护航。当然，目前的Q-SASE整体方案还处于初级阶段，仍需要通过不断的研究及技术实现，将现有的安全能力以及未来可能增加的安全能力通过编排集成到一起，并且实现安全能力编排化、安全流程自动化、安全运行智能化的升级演进。

参考文献

[1] Gartner. The future of network security is in the cloud [R]. 2019
[2] Gartner. SASE will improve your distributed security everywhere [R]. 2020
[3] Gartner. 2021 strategic roadmap for SASE convergence [R]. 2021
[4] MEF70. SD-WAN service attributes and services [EB/OL]. [2022-11-25]. https://www. mef. net/wp-content/uploads/2019/07/MEF-70. pdf? id=122&fileid=file1
[5] 云安全联盟大中华区. SASE安全访问服务边缘白皮书 [R]. 2022
[6] CCSA. 安全访问服务边缘(SASE)能力成熟度: T/ZGTXXH 048 [S]. 2022

作 者 简 介

王茜，奇安信科技集团SASE产品部总经理、中国通信学会第八届信息通信网络专家委员会委员；先后在中国电信北京研究院、中国电信集团公司、奇安信科技集团从事网络规划与优化、新技术新产品研究等工作，曾参与ITU-T SG13、MEF、IETF等标准工作；有40余篇标准文稿被采纳，发表论文30余篇，出版专著5本，获授权专利6项。

陈晨，奇安信科技集团助理总裁、中国软件行业协会信息主管（CIO）分会副主任委员；负责奇安信科技集团信息管理部的管理工作，先后在中国国航、香港航空、奇安信科技集团从事信息化与数字化管理工作，曾参与《数字化管理师能力评估标准》团体标准的编写与制定工作。

井俊丰，奇安信科技集团总体部网络安全架构师；从事网络安全规划与架构设计、网络安全解决方案与落地支撑等工作，主持或参与多个“十四五”网络安全规划设计与工程落地建设工作。

季家震，奇安信科技集团SASE产品部产品经理；从事SASE产品规划及设计工作。