 DOI: https://doi.org/10.12349/iser.v7i1.9033

Application and Innovation of Cloud Security Based on SaaS Model in Small and Medium-sized Enterprises

Yajun Zhu

Zhenjiang Branch of China Mobile Communications Group Jiangsu Co., Ltd., Danyang, Jiangsu, 212300, China

Abstract

This study utilizes China Mobile Cloud's cloud security technology and the practical cybersecurity incident response experience of Danyang Municipal Cyberspace Administration to explore the application of cloud security SaaS services in various scenarios for small and medium-sized enterprises (SMEs). Characterized by lightweight, high efficiency, and cost-effectiveness, these services are particularly suitable for typical digital economy scenarios such as ransomware protection, data security, and endpoint defense for SMEs. Effectiveness evaluations demonstrate that this model significantly reduces malware infection rates, decreases the likelihood of data breaches and ransomware attacks, while substantially shortening security incident response times. Through the integration of theoretical analysis and practical implementation, we have developed this methodology, providing SMEs with effective technical references and actionable solutions for digital economy security.

Keywords

SaaS; cloud security; mobile cloud; cloud-network integration

基于 SaaS 模式的云安全在中小企业的技术应用与创新探索

朱亚俊

中国移动通信集团江苏有限公司镇江分公司，中国 · 江苏 丹阳 212300

摘　要

此文基于中国移动云的云安全技术，结合丹阳市网信办的实际网络安全事件处置经验，本文研究云安全SaaS服务在中小企业多场景下的应用，云安全服务具有轻量化、高效率、低成本的特征，适宜于数字经济背景下中小企业勒索病毒防护、数据安全和终端防护等典型场景，效果评估显示，这个模式能显著降低恶意软件感染率，它减少了数据泄露和勒索病毒的发生概率，同时显著缩短了安全事件的响应时间。通过理论和实践的结合，我们归纳出这套方法，为中小企业数字经济安全提供了有效的技术参考和实施方案。

关键词

SAAS；云安全；移动云；云网一体

1 引言

在数字经济时代，中小企业面临勒索病毒威胁、数据安全隐患和信息泄露等多重数字安全风险，以往基于硬件部署和本地运维的传统安全防护方法存在灵活性不足、运维成本昂贵、响应延迟等挑战，这些手段已经不足以满足中小企业对轻量化、高效率、低成本安全能力的核心要求，此文着重研究 SaaS（Software as a Service）云安全。SaaS 具有按需订阅、快速部署、集中运维的特性，文章分析了它在勒索病毒防护、数据安全、终端防护等场景的应用，这种模式能降低资源支出，它还可以提供全链路的安全防护能力，这为中小企业建立新的安全体系提供了有效的解决方案，文章分析了当前模式的缺陷之处，阐述了未来发展的潜在性，目的是为中小企业安全建设探讨有效的技术方案和实施方法。

【作者简介】朱亚俊（1983–），中国江苏丹阳人，本科，工程师，从事云业务、大数据、物联网在行业信息化中的应用研究。

2 中小企业网络安全现状与问题分析

2.1 中小企业主要网络安全威胁

当前，中小企业的数字经济

发展既面临着机遇，也充满挑战，其中之一便是网络安全风险，主要威胁可归纳为以下几类：

恶意软件：由于员工终端因访问非法网站或打开钓鱼邮件，易引入病毒、木马、蠕虫等恶意程序，可能导致系统瘫痪或数据窃取，严重情况下还会影响网络的正常运行。

勒索软件：攻击者通过漏洞利用或社会工程手段加密核心业务数据，索要赎金，这对企业生存构成严重威胁。

数据泄露：因数据库配置错误、API 接口暴露或内部

人员误操作，客户信息、财务数据等关键资产易遭被非法获取，引发合规风险与品牌声誉损失。

2.2 传统网络安全防护方案的缺失

在数字经济边界特征已从传统的封闭局域网，演变为业务上云、数据跨域流动、终端泛在化（涵盖 IOT 设备、移动终端）以及 AI、大数据、区块链等新技术的广泛应用。传统依赖“城堡 - 护城河”式边界防护的模式，难以实现对动态、泛在风险的持续可见与有效控制。

与此同时，数字经济环境下的业务迭代速度显著加快，多地协同成为常态，这对安全体系的敏捷部署与策略调整能力提出了更高要求。然而，传统防护模式普遍依赖一次性硬件采购，部署周期往往以周或月计，策略变更亦需现场操作，难以及时响应业务的快速变化。

此外，电商大促、直播带货等新业态普遍具有流量突发性强、峰值波动大的特点。传统安全方案多基于固定性能的硬件设备构建，面对流量激增时易出现性能瓶颈，甚至在吞吐能力不足时导致防护策略失效或业务中断，直接影响业务连续性与用户体验。

3 移动云云安全解决方案能力和特点

调研显示，传统防护模式在架构边界、资源投入、部署效率与弹性能力等方面均难以匹配中小企业数字数字经济背景下的安全需求。针对以上痛点，移动云提出“云 - 网 - 边 - 端”协同的 SaaS 化云安全架构，实现从终端接入到数据运营的全链路防护，支持按需订阅、弹性扩展与统一运维。

3.1 云安全技术和重要能力

3.1.1 云网融合的安全能力

云网融合的核心在于打破网络与安全的割裂状态，实现“网随算动、算网一体”的一体化防护与调度，从而提升安全策略与网络资源的协同效率。

云网安一体化接入：通过 SASE 架构，将安全 Web 网关（SWG）、云访问安全代理（CASB）、零信任访问与云端安全能力融合，对总部、分支及移动办公的访问流量进行统一纳管，实现上网行为管控、应用识别与策略统一，并以云原生方式轻量交付，显著简化多设备、多分支场景的运维工作。

统一编排与算网大脑：依托自研“大云”操作系统与算网大脑，实现异构算力并网与云网资源的统一编排，使云网服务可做到一点接入、即取即用，在安全与网络能力之间建立高效的联动通道。

高可用与就近防护：结合“N+31+X”与 3000 余个边缘节点的广域覆盖，以及云专网与多 AZ 资源池，提供路径可视、故障快速倒换与就近清洗 / 防护能力，确保跨域与高并发业务场景下的安全与连续性。

3.1.2 云边协同的安全能力

云边协同旨在将安全能力延伸至业务最近侧，缩短威胁检测与处置的路径，特别适合工业现场、园区、CDN/ 视频、物联网等对低时延与本地化合规有较高要求的场景。

分布式云与边缘算力：采用“大区制中心节点 + 分布式边缘架构”匹配国家“东数西算”8 大枢纽布局，已在全国上线 33 个直管资源池、13 个中心节点、16 个省级节点、3000 个边缘节点，使安全能力可贴近业务发生地部署。

边缘安全托管：在边缘侧布设轻量化安全代理或网关，与云侧统一策略编排联动，实现终端—边缘—云三级的威胁检测、联动处置与日志统一回传，满足本地化合规与低时延需求。

统一安全运营：以态势感知 +SOAR 实现跨域安全事件的关联分析与自动化响应，配合云堡垒机与日志审计，满足多租户、多分支的合规审计与取证要求；在重大活动与关键时期，可提供 7×24 小时属地化快速响应。

3.2 云安全 SaaS 服务特点

云端软件服务（SaaS）是一种创新的软件交付模式，它将应用程序部署于远程服务器，让用户能够通过网络获取所需功能。

在中小企业云安全领域的实践中，这一方案有效化解了本地部署方式带来的资源浪费、运维开销巨大以及安全策略更新不及时等难题，特别适合预算受限且技术实力不足的中小型企业。

基于云端托管和即时接入的特点，移动云安全服务能够在不大幅改动现有系统架构的情况下，快速部署网站防护功能，大幅缩减防护体系的建设周期。系统可根据业务负载的起伏自动调节防护规模，有效应对电商大促、在线直播等高访问量场景，确保安全防护效果和业务持续运营。

此外，通过将安全功能细分为独立模块并支持灵活订购，中小企业可以先从基础防护开始，随着业务发展逐步增加或升级所需的安全组件。这种方式既能避免业务淡季时的资源闲置，又可在业务扩张期快速获取所需的安全保障，实现了资源效益和投入成本的最优配置。

4 云安全在中小企业重点应用场景

在数字经济背景下，不同行业及业务形态所面临的网络安全威胁呈现出显著的差异化特征。为有效应对复杂多变的安全风险，以下结合实际应用，重点阐述三大典型场景下的安全挑战与应对策略。

4.1 智能工厂边界安全防护体系构建

解决痛点：中小企业普遍面临网络防护能力薄弱的问题：其一，网络边界划分模糊，生产网与办公网未进行有效隔离，易形成攻击传导路径；其二，缺乏专业安全监测工具，难以实现全局态势感知，对勒索病毒、工控协议攻击及横向渗透等威胁的发现与响应滞后；其三，传统硬件防护部署成本高、运维复杂，与中小企业资源禀赋不匹配。

方案应用： 在企业网络出口侧部署专线安全卫士，集

成下一代防火墙（NGFW）、入侵防御系统（IPS）等安全功能模块，实现网络层与业务层的双重边界防护。依托云端移动云安全运营平台的智能算法对流量、设备行为及协议特征进行多维度分析，实现威胁态势预测与实时预警。当检测到攻击行为时，系统可自动生成并下发阻断策略至边缘防护设备，完成“检测—分析—响应”闭环。

4.2 Web 业务安全场景

解决痛点：中小企业的线上电商交易平台直接面向公网，易遭受 SQL 注入、跨站脚本攻击（XSS）、CC 攻击等 Web 应用层威胁；在业务高峰期，流量激增易导致防护性能不足，进而引发交易中断、数据泄露或客户信息被爬取。

方案应用：采用 SaaS 化 Web 应用防火墙（WAF）与云原生下一代防火墙相结合的防护架构。该方案具备弹性伸缩能力，可根据实时流量动态调整防护资源，有效抵御各类 Web 层攻击，满足中小企业对成本效益与安全性能的双重需求。

4.3 勒索病毒综合防护

解决痛点：中小企业普遍面临基础防护薄弱、攻击入口多、勒索病毒防不住、备份缺失或失效、业务恢复难救不回、专业能力匮乏、处置效率低响应慢等问题。

方案应用：使构建“预防—检测—恢复”三位一体的勒索病毒综合防护体系。首先，依托云存储与云备份服务，建立自动化、周期性的数据备份策略；其次，在网络边界部署具备多引擎病毒查杀、入侵防御（IPS）、僵尸网络识别与阻断能力的“专线安全卫士”，从入口层面阻断初始攻击载荷；最后，结合云端安全运营中心（SOC）提供 7×24 小时威胁监测与专家级应急响应支持，全面提升中小企业的主动防御与灾后恢复能力。

5 移动云安全在中小企业的实践验证与前景研究

5.1 应用效果量化评估与实证分析

为验证所提云 sass 安全解决方案的实际效能，结合参与丹阳市网信办网络安全事件处置的实践，在 2023 年至 2024 年期间，对 106 家制造、电商及服务类中小企业开展试点部署，并采集关键运行数据进行量化评估。

表 1：SaaS 云安全部署前后效果对比

	实施前	实施后	改善率
恶意软件感染率	20.6%	5.5%	73.3%
数据泄露	10 起	0 起	100%
勒索病毒	5	0	100%
安全事件响应时间	平均 5H	平均 30min	90%

注：改善率 =（实施前 − 实施后）/ 实施前 × 100%

典型案例场景效果佐证：

某眼镜制造企业在部署专线安全卫士+云备份体系后，成功拦截一起利用 SMB 协议漏洞的勒索病毒横向渗透攻击。系统在 3 分钟内完成告警、策略下发与网络隔离，避免约 200GB 生产图纸数据被加密。

5.2 未来应用前景与发展方向

在当前人工智能技术不断革新的背景下，云安全也需通过人工智能赋能。将大语言模型、机器学习算法等人工智能技术深度融合到 SaaS 云安全体系中，在威胁检测、漏洞挖掘、态势感知与自动化响应（SOAR）等场景中，深度应用大模型与智能体，这种整合促进中小企业的安全运营模式逐步从传统 的“人工主导的分析研判”向”智能助理驱动的自动化处置”转变，这一转变不仅有效降低了中小企业安全运营的技术门槛与人力成本，还在高频网络威胁场景中实现更快速、更精准的安全响应。

5.3 局限性与未来工作展望

尽管基于 SaaS 模式的云安全技术在中小企展现出显著优势，其“通用化”特性反而可能成为制约因素。制造、医疗、教育、电商等行业的安全需求差异明显，不同行业对数据安全与隐私保护的合规要求差异显著。未来 SaaS 云安全将向行业化模板发展，如工业协议深度检测、医疗数据隐私合规包、教育网络安全准入包等，实现“一键适配”。

6 结语

本文针对中小企业安全困境，提出“云 - 网 - 边 - 端”协同 SaaS 架构，融合云网融合、云边协同，构建“预防—检测—恢复”防护体系，实现跨域弹性防护与按需订阅。实证显示，试点企业恶意软件感染率降 73.3%，勒索病毒与数据泄露零发生，响应时间缩 90%。创新在于架构突破、技术融合及轻量化应用模式，为中小企业提供高性价比安全方案，未来将深化 AI 与行业化适配，助力行稳致远。

参考文献

[1] 邹莉萍 & 邹莉强.(2025).基于云计算技术的网络安全防御技术研究.哈尔滨职业技术学院学报,(06),92-94. https://doi.org/10.16145/j.cnki.cn23-1531/z.2025.06.007.

[2] 迟江波 & 殷珊.(2025).计算机网络安全的前沿防护策略研究.电脑知识与技术,21(21),61-63. https://doi.org/10.14004/j.cnki.ckt.2025.1041.

[3] 张怡晨.(2025).基于算网融合背景下的云安全管理及防护测评研究.通信与信息技术,(02),80-84.

[4] 冯云婷,李攀,李景景 & 刘紫阳.(2025).电子信息工程中网络安全技术应用研究.软件,46(02),4-6.

[5] 何文康,秦余芬,聂耀峰 & 刘烨.(2025).基于等级保护2.0标准的公有云上业务安全测评研究与实践.网络安全技术与应用,(02),72-77.