文章类型：论文|刊号（ISSN）：2972-4007(P) / 2972-4015(O)

客户需求驱动的网络安全企业服务模式创新研究

徐彬　伍海燕　仉进　夏晓雨　杨梦格
安徽信科共创信息安全测评有限公司
DOI:10.32629/deitar.v4i2.22310

[摘　要] 数字化业务持续向云平台、移动终端、工业互联网和数据要素流通场景延伸,网络安全需求已经由相对单一的边界防护逐步转向覆盖业务运行、数据流转、风险监测和应急处置的综合安全保障。传统以安全设备销售和项目制交付为核心的服务模式,容易出现需求识别不深、产品配置与业务场景脱节、服务连续性不足、价值评价偏技术指标等问题,难以适应客户安全需求动态化和长期化的发展趋势。
[关键词] 客户需求；网络安全企业；安全服务；持续运营
中图分类号：TP393.08　文献标识码：A

Research on the Innovation of Security Network Enterprise Service Model Driven by Customer Demand

Bin Xu　Haiyan Wu　Jin Zang　Xiaoyu Xia　Mengge Yang
Anhui Xinkexin Co-Create Information Security Testing Co., Ltd.

[Abstract] Digital business is continuously extending to cloud platforms, mobile terminals, industrial internet, and data element circulation scenarios. The cybersecurity requirements have gradually shifted from relatively simple boundary protection to comprehensive security guarantees covering business operation, data flow, risk monitoring, and emergency response. The traditional service model centered on the sale of security equipment and project-based delivery is prone to problems such as insufficient demand identification, mismatch between product configuration and business scenarios, insufficient service continuity, and biased value evaluation towards technical indicators, making it difficult to adapt to the dynamic and long-term development trend of customers' security needs.
[Key words] Customer needs; Cybersecurity enterprises; Security services; Continuous operation

引言

数字化转型不断改变企业的信息系统架构和业务运行方式,云计算、移动办公、工业互联网、物联网以及数据跨系统流动扩大了网络安全风险的暴露范围。客户采购网络安全产品的目标也发生明显变化,单纯购买防火墙、入侵检测、终端防护等产品已经不能完整解决业务连续性、数据保护、攻击处置和合规治理问题。越来越多客户开始关注安全能力能否持续运行、风险能否及时发现、事件能否形成闭环处置,以及安全投入能否真正降低业务风险。2023年1月,工业和信息化部等十六部门印发《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》(工信部联网安〔2022〕182号),明确提出提升数据安全产品和服务供给能力,深化重点行业领域应用,推动产业生态和创新体系建设。

1 客户需求驱动服务创新的内在逻辑

1.1安全需求由合规建设转向风险治理

网络安全市场早期需求具有较强的合规驱动特征,客户往往依据等级保护、安全检查或者行业监管要求采购相关设备和服务。在这种需求结构下,网络安全企业通常按照制度要求形成产品清单,完成设备部署、策略配置和项目验收后即可结束主要服务过程。随着攻击手段、业务架构和数据流转方式不断变化,仅满足静态合规要求已难以覆盖真实风险。当前客户更加关注安全事件是否能够发现、异常行为是否能够识别、重要业务遭受攻击后能否快速恢复等实际问题。合规仍然构成安全建设的重要基础,但客户需求逐渐从“是否部署安全措施”转向“安全措施是否真正有效”。例如,终端安全产品部署完成并不意味着勒索软件风险得到有效控制,客户还需要掌握终端资产状态、补丁缺口、异常进程、横向移动以及处置时效。

1.2技术需求由单点防护转向体系协同

传统网络安全建设通常按照网络边界、终端、服务器、数

Copyright © This work is licensed under a Commons Attribution-Non Commercial 4.0 International License.

文章类型：论文|刊号（ISSN）：2972-4007(P) / 2972-4015(O)

据库等对象分别配置安全产品，各产品能够解决特定领域的问题，但不同产品之间的数据标准、告警机制和处置流程可能相互独立。客户规模较小时，单点产品能够满足基础防护要求；随着信息系统复杂度提高，碎片化产品越来越容易造成告警分散、数据孤立和重复建设。客户关注重点因此逐渐从单项产品性能转向整体安全能力。例如，一次异常登录事件可能同时涉及身份认证、终端行为、网络访问、数据调用和业务系统日志。如果不同安全设备独立运行，安全人员需要人工关联多个平台的信息，不仅影响判断效率，也容易遗漏关键线索。客户真正需要的是资产、身份、流量、终端、应用和数据之间能够形成关联分析，使风险发现和事件处置能够在统一逻辑下运行。

1.3服务需求由项目交付转向持续运营

网络安全风险具有明显的动态特征。新的资产不断上线，应用版本持续更新，员工账号和权限发生变化，漏洞持续出现，攻击者的技术手段也在调整。项目验收时处于安全状态的系统，并不能保证数月后仍然维持相同风险水平。因此，一次性建设和阶段性检测越来越难以匹配客户安全需求。客户开始关注安全能力运行过程，希望网络安全企业持续提供资产梳理、漏洞监测、威胁分析、告警研判、应急响应和安全策略优化等服务。特别是自身安全团队规模有限的中小企业，以及存在大量生产系统、分支机构和云上资产的客户，更倾向于引入外部专业力量承担部分安全运营工作。

2 网络安全企业服务供给的现实困境

2.1需求识别仍停留于技术清单

部分网络安全企业开展售前交流时，仍然按照已有产品体系反向寻找客户需求。需求调研集中在设备数量、网络带宽、终端规模、接口类型和部署方式等技术信息，对客户核心业务、关键数据、风险承受能力以及安全组织现状了解不足。由此形成的方案虽然技术配置完整，却未必能够解决客户最迫切的问题。客户提出“加强数据安全”“建设安全运营中心”等要求时，其背后可能存在不同诉求。有的企业主要面临外部攻击，有的企业希望控制内部数据泄露，有的企业需要提高安全事件处置效率。如果网络安全企业不进一步拆解需求，就容易按照标准模板提供相似方案，使安全建设出现功能过剩或者关键能力缺失。需求识别不足还容易导致方案频繁变更。

2.2产品交付与业务场景存在脱节

网络安全产品具有较强专业性，但安全技术只有嵌入具体业务场景才能形成实际价值。现实项目中，一些企业重视设备上线和功能启用，却没有充分考虑客户业务系统的访问规律、运维流程和生产要求。例如，过于严格的访问控制可能影响正常业务，告警策略缺乏场景调优则可能产生大量低价值告警，安全平台即使能够采集海量日志，也不一定能够帮助客户快速判断真实攻击。场景脱节的根源在于服务设计仍然以产品功能为中心。技术人员更熟悉设备能力，却未必了解客户核心业务链条。当安全要求和业务运行出现冲突时，如果企业无法准确判断哪些业务需要重点保护、哪些操作属于正常行为，就只能采取较为保守的配置方式。服务模式创新需要改变这种状况。

2.3服务过程缺乏运营闭环

许多安全服务已经包含漏洞扫描、监测预警、应急响应等内容，但不同服务之间仍可能相互分离。漏洞扫描形成报告后缺少整改跟踪，告警推送给客户后没有确认处置结果，应急事件处理完成后也未必将经验转化为新的检测规则。服务活动数量较多，却没有形成持续改进机制。安全运营真正有效的关键并非发现多少告警，而是风险能否形成“发现—研判—处置—验证—优化”的闭环。如果漏洞反复出现、同类攻击持续触发、异常账号长期得不到处理，说明运营工作仍停留在信息传递阶段。客户需要的是问题得到控制，而不仅是收到报告。网络安全企业在服务过程中还需要建立明确的责任接口。哪些风险由服务商直接处理，哪些需要客户业务部门配合，重大事件由谁决策，整改超过时限后怎样升级处理，都应在服务体系中明确。

2.4价值评价偏重技术指标

传统网络安全项目通常使用设备上线率、策略配置数量、漏洞发现数量、告警数量等指标评价服务效果。这些数据便于统计，却不能完整说明客户获得了多少安全价值。告警数量较高可能来自攻击增多，也可能来自规则质量不高；漏洞发现数量较多不代表风险降低，如果整改率长期偏低，检测本身很难产生完整价值。客户更关心安全投入对业务产生的实际影响，例如高危漏洞暴露时间是否缩短，重大安全事件能否快速发现，核心业务是否因攻击出现中断，处置过程是否减少损失。网络安全企业如果仍然以技术工作量证明服务价值，很难建立长期稳定的客户关系。价值评价需要由“做了多少工作”转向“解决了多少问题”。企业可以结合风险闭环率、重大风险平均处置时间、重复事件发生率、关键资产覆盖率、服务可用性等指标评价运营效果，并将技术指标与客户核心业务风险联系起来。

3 客户需求驱动的网络安全企业服务模式创新路径

3.1建立需求分层和场景画像机制

客户需求驱动并不意味着被动接受客户提出的所有技术要求，而是将客户表层需求进一步转换为可执行的安全目标。网络安全企业可以建立需求分层模型，将客户需求划分为合规需求、业务连续性需求、攻击防御需求、数据保护需求和运营效率需求，并根据行业属性、资产规模、技术架构和安全能力成熟度确定服务重点。需求调研应从传统设备调查扩展到业务调查。项目启动阶段需要识别客户关键业务系统、重要资产、敏感数据、主要外部接口、人员权限关系和第三方访问情况，形成业务资产画像。在此基础上进一步构建风险场景，例如账号被盗后的异常登录、外部漏洞利用后的横向移动、敏感文件异常下载以及关键业务遭受拒绝服务攻击等。场景画像能够将抽象安全需求转化为具体服务内容。

3.2重构咨询建设运营融合服务链

客户安全需求贯穿规划、建设和运行全过程，网络安全企业

Copyright © This work is licensed under a Commons Attribution-Non Commercial 4.0 International License.

文章类型：论文|刊号（ISSN）：2972-4007(P) / 2972-4015(O)

应改变咨询、产品交付和安全运营相互割裂的服务结构。咨询阶段形成的风险分析应直接进入方案设计，建设阶段形成的资产和策略信息应继续用于运营，运营阶段发现的问题又应推动原有安全体系持续调整。在咨询环节，企业需要帮助客户明确安全目标和建设优先级，而不是简单形成产品采购建议。通过资产梳理、风险评估和安全能力差距分析，确定哪些风险需要技术控制、哪些需要流程调整、哪些可以通过运营服务解决。建设环节则围绕这些目标完成安全能力配置，并为后续运营预留数据接口、日志采集和联动处置能力。运营阶段成为服务链的重要延伸。安全企业需要持续采集资产状态、漏洞信息、终端行为、网络流量和安全告警，对风险进行关联分析。当发现新的攻击方式或者客户业务结构变化时，应及时调整检测规则和防护策略，使服务能力随风险变化而更新。

3.3推进平台化和订阅化服务供给

持续性安全需求要求网络安全企业改变高度依赖现场人员的交付模式。对于资产监测、漏洞发现、告警分析、威胁情报和日志运营等具有持续性特征的服务，可以通过统一安全运营平台实现集中化供给，在客户侧保留必要的数据采集和响应能力，由服务平台承担分析和运营任务。平台化并不等于将所有客户数据集中存储，而是通过标准化接口、统一运营流程和分级权限机制提高服务效率。对于具有数据本地化要求的客户，可以采用本地部署平台与远程运营团队协同的方式，在满足数据控制要求的同时获得专业运营能力。大型客户可以建立专属安全运营体系，中小客户则可以使用共享型托管安全服务，降低安全能力建设门槛。商业模式也可以由一次性项目收入逐步向订阅式服务收入延伸。企业可按照资产规模、服务范围、响应等级和运营深度设计不同服务套餐，将安全监测、风险分析、应急响应和专家支持组合形成周期性服务。

4 结语

网络安全产业的竞争正在由单一产品能力竞争逐步延伸至综合服务能力竞争。客户安全需求具有动态性、场景性和持续性，传统依赖设备销售和项目交付的服务模式难以完整覆盖业务运行中的长期风险。网络安全企业需要将客户需求作为服务模式设计的起点，把业务场景和风险目标嵌入咨询、建设、运营和评价全过程。客户需求驱动并不是简单提高定制化程度，而是建立能够持续识别需求、配置能力、评价效果和优化服务的运行机制。通过需求分层和场景画像，可以提高安全方案的针对性；通过咨询、建设和运营衔接，可以形成完整服务链；通过平台化和订阅化供给，可以增强持续服务能力；通过价值共创和闭环评价，可以使安全投入与业务风险治理形成更加清晰的联系。

[参考文献]

[1]袁飞晖,曾晖,骆小凡.远洋客船网络化服务平台安全防护需求与安全管理[J].珠江水运,2023(12):96-98.

[2]陆世将.基于“互联网+”的造修船企业安全管理方法的创新探究[J].中国修船,2025,38(S1):71-73.

[3]黄耀文,陈龙如.差异化拓展安全防护市场,安全大脑助力企业保存拉新[J].广东通信技术,2023,43(1):2-7.

[4]樊华.探究现代企业网络安全建设新模式[J].中国新通信,2023,25(23):116-118.

[5]付凯艳,孙博.现代化钢铁企业网络安全管理体系的建设[J].河北冶金,2023(S01):71-75.

作者简介：

徐彬(1989--),男,汉族,安徽省池州市东至县人,本科,网络安全等级保护测评师证书(中级),主要研究方向：计算机科学与技术。

Copyright © This work is licensed under a Commons Attribution-Non Commercial 4.0 International License.