云安全平台升级项目

可行性研究报告

网宿科技股份有限公司

2023 年 1 月

目 录

第一章 项目概况

一、项目名称

云安全平台升级项目。

二、项目简介

网宿科技股份有限公司（以下简称“网宿科技”或“公司”）拟使用部分非公开发行股票募集资金，建设云安全平台升级项目（以下简称“安全升级项目”）。该项目基于公司遍布全球的边缘安全节点及庞大的带宽储备，建设一个即开即用、模块化开启的 WAAP 平台，为面向公众的 Web 应用程序、API、APP、H5、小程序等提供全面的保护。

三、项目投资主体

本项目建设主体为公司及公司全资子公司香港申嘉科技有限公司、厦门网宿有限公司。

网宿科技成立于2000年1月，致力于成为全球领先的IT基础平台服务提供商。通过提供计算、存储、网络及安全等新一代信息技术服务，助力互联网客户、政府及企业客户获得快速、稳定、安全的IT能力和用户体验。近几年，公司围绕信息技术基础设施平台能力建设，围绕解决、助力互联网及政企客户数字化、智能化转型中的IT需求拓展自身业务，在CDN、IDC等成熟业务的基础上，正在进行向“云安全”与“边缘计算”方向的革新，推进全球化边缘计算平台和安全访问边缘架构建设，不断完善平台能力；并积极拓展私有云/混合云、MSP、数据中心液冷解决方案等新业务。

公司通过全资子公司香港网宿科技有限公司间接持有香港申嘉科技有限公司（以下简称“香港申嘉”）100%股权，在公司海外业务开拓总体规划下，通过香港申嘉进行项目海外部分的实施。另外，公司持有厦门网宿有限公司（以下简称“厦门网宿”）100%股权，由厦门网宿承担部分研发职能。

第二章 项目建设内容和建设必要性

一、项目建设内容

1、建设内容

基于公司遍布全球的边缘安全节点及庞大的带宽储备，建设一个即开即用、模块化开启的 WAAP 平台，为面向公众的 Web 应用程序、API、APP、H5、小程序等提供全面的保护。WAAP 平台在提供 WAF 功能的同时，解决了传统 WAF 被动式响应和滞后性防护的困局，并能够抵御或有效缓解大流量 DDoS 攻击、智能化爬虫攻击和因 API 滥用导致的负面影响。通过统一的

平台、统一的入口实现一站式的防护，通过全流量分析与日志聚合，实现用户访问及攻击数据的追踪和透视。

2、对现有平台、产品的改进

云安全平台升级后，可以实现：

（1）安全管理闭环，通过统一的 WAAP 平台实现多维度攻防数据的聚合分析及统一处置，实现安全管理闭环；

（2）自适应防护，自动化地根据请求或流量数据的不同特点动态改变防护逻辑，有效提升防护的精细度和准确度；

（3）威胁情报升级，基于网宿安全平台海量攻防样本，实现高覆盖、及时及可解释性强的情报管理和情报生产体系，满足各个安全模块的共同能力，提高防护效率和准确性；

（4）客户操作体验优化，对于新客户，提供即开即用的防护策略模板，对于专业客户，提供多维度个性化配置，保障不同专业程度的客户实现精细化安全运营的效果；

（5）海外交付能力增强，通过本地化的资源、服务和运营系统，搭建完善的本地化交付体系，助力拓展海外安全市场。

另外，对目前产品及解决方案的改进具体如下：

现有产品	本项目实施内容	相对现有产品（解决方案）的改进
DDoS 云清洗	场景化防护性能提升	1、根据业务受攻击情况及业务优先级智能调整防护节点覆盖，实现业务攻击防护效率提升与用户访问性能提升二者兼得； 2、网络层/应用层全场景防护能力增强。
Web 应用防火墙	Web 防护策略优化与管理	1、场景化防护适配：在原有的场景化策略模板基础上提供更多场景配置，例如网络安全重保场景、夜间场景、节假日场景等，确保防护策略与业务场景最大程度适配； 2、基于网宿在各行业的安全运营经验及不同行业业务特性提供行业策略模板配置； 3、AI 模型持续优化，攻防基因注入 AI 模型，提高 WAF 防护能力。
Bot Guard 爬虫管理	AI 防护与动态对抗	1、全场景防护能力增强，增强在 Web/App/小程序端的防护能力，自动识别不同客户端环境并适配相应的防护策略； 2、ML 驱动的启发式（主动）检测，加强对 APBs（Advanced persistent bots）的管控能力； 3、动态对抗引擎升级，实现业务全流程检测并加强反调试、反破解能力，全面封堵 Bots 黑灰产。

API 安全与管理	基于业务与数据视角的 API 安全治理平台	1、以 API 自身及其所承载应用与业务的整体安全为目标，通过 API 资产梳理、API 定义、API 风险识别（包含风险暴露面如漏洞等、风险事件）、API 防护（API 自身：合规检查；应用安全：DDoS 和 Web 漏洞防护；业务安全：Bots 防护），实现 API 安全完整闭环； 2、以数据为中心，提高敏感数据自动识别、分类分级能力，同时搭载丰富、易用的管理工具，助力客户数据安全治理。

3、建设目标

（1）进一步提升安全产品智能化、自主化

随着网络攻击朝着规模化、产业化、智能化的方向迈进，公司将加大 AI 研究的投入，将多年攻防经验及多行业客户运营经验注入 AI 模型，打造智能、自适应、持续进化的 AI 防护能力，以 AI 撬动攻防天平，提升产品的核心竞争力，保持公司在安全防护能力和理念上的持续领先。

（2）建立可见、可选的安全能力平台，更好的支持客户业务拓展

公司将安全能力以模块化或模板化的方式提供给客户，满足不同阶段客户的个性化防护需求。模块化的方式支持为客户提供精细化配置的能力，根据安全模块、防护对象的不同自由组合防护策略，提升安全策略与业务的契合度；另外，模板化的方式支持为客户提供即开即用的能力，可一键复用网宿安全运营专家在不同业务场景和行业中的多年积累。

（3）完善安全底座，支持公司安全业务发展

持续深耕安全攻防技术，构建深厚的安全资源池与能力池，夯实安全底座，基于此为客户的互联网应用提供一站式的 WAAP 服务，为企业应用访问/远程办公提供零信任安全接入服务，并以此为基础助力安全产品线拓新业务良性发展。

二、项目建设必要性

1、网络攻击持续增长，安全能力愈发重要

近年来，各类网络攻击和数据泄露事件层出不穷，安全形势日益严峻。根据 CNCERT《2021 年上半年我国互联网网络安全监测数据分析报告》数据显示，2021 年上半年，国家信息安全漏洞共享平台（CNVD）收录通用型安全漏洞 13,083 个，同比增长 18.2%；“零日”漏洞收录数量为 7,107 个（占 54.3%），同比大幅增长 55.1%。监测发现，境内外 8,289 个 IP 地址对我国境内约 1.4 万个网站植入后门，我国境内遭篡改的网站有近 3.4 万个，其中被篡改的政府网站有 177 个。

另外，在边缘计算时代，安全能力愈发重要。边缘计算赋予企业将业务前移的能力，使云中心的业务能力下放到网络边缘，与此同时网络攻击战场也更加分散化、前置化，边缘计算的发展必须以边缘安全为坚实后盾，安全与业务需同步建设、同步规划、同步运营。

2、安全市场前景广阔

2021 年 3 月， 国家发布《“十四五”规划和 2035 年远景目标纲要》，规划中专门提出全面加强网络安全保障体系和能力建设，把网络安全与人工智能、大数据、区块链、云计算共同列为 5 大新兴数字产业，明确要求培育壮大，加快推动。

2021 年 7 月，工信部发布《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》，目标是到 2023 年，网络安全技术创新能力明显提高，产品和服务水平不断提升，经济社会网络安全需求加快释放。

中国网络安全产业联盟（CCIA）发布的《中国网络安全产业分析报告（2022 年）》数据显示，2021 年我国网络安全市场规模约为 614 亿元，同比增长率为 15.4%。近三年网络安全行业总体保持增长态势，随着《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》、《网络安全审查办法（2021 年修订）》颁布实施，网络安全法律法规体系化、纵深化态势更加明显，政策法规红利持续释放，叠加企业和个人数字化需求不断攀升，网络安全市场持续扩大，预计未来三年增速仍将保持在 15%以上，到 2024 年市场规模预计将超过 1,000 亿元。

根据Gartner发布的《Web应用程序和API保护魔力象限》：到2024年，70%实施多云战略的企业将青睐云 Web 应用程序和API保护平台 （WAAP） 服务，而不是WAAP设备和IaaS原生WAAP；到2026年，40%的企业将根据API保护以及Web应用程序安全功能选择WAAP提供商，而2022年这一比例不足15%;到2026年,超过40%拥有面向消费者的应用程序的企业,将依靠WAAP来缓解僵尸攻击，2022年该比例不到10%。

3、增强公司安全能力、支持更多业务场景

安全业务是公司重要业务布局方向之一。网宿安全以“连接、可靠、共进”为主旨，致力成为智能边缘安全领导者。公司客户群体覆盖政府机关、金融、交通、零售、航空、电子商务等领域,补齐公司安全能力,提升不同业务场景下的防护效率不仅是作为服务商的责任，更是社会责任与使命。

第三章 项目可行性分析

一、政策支持安全行业发展

我国相继出台《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》等网络安全法规/政策，公众对信息安全的重视程度得到提升，为国内整体网络安全市场的高速发展提供了政策保障、为网络安全行业注入了新活力。对企业而言，安全事件的代价和后果早已不可同日而语，在大趋势下企业必然增加安全投入。

二、公司在安全领域的积累，为项目建设提供有力保障

网宿在全球拥有广泛部署的安全加速节点，庞大的节点数量为客户构建安全护城河，边缘防护架构使“战场”远离源站，以自身的资源优势撬动安全攻防的天平，为客户化解来势汹汹的攻击。网宿平台日均缓解数十亿次攻击，海量攻防样本不断反哺防护策略模型，实现持续进化的智能防护。另外，公司拥有服务各行各业的丰富经验，并且在诸多大型活动期间承担网络安全重保工作，经验丰富。

在人才储备方面，目前，公司网络性能及安全事业部的研发及技术人员超过200人，均具有丰富的研发经验，公司将根据研发需要在本项目实施过程中扩充研发队伍，保障项目的顺利实施。

另外，经过二十多年的深耕细作，网宿科技积累了丰富的客户资源、广泛的合伙伙伴，在销售网络、市场品牌等方面建立了较强的竞争优势，能保障本项目研发成果的转化。

三、项目资金的有效保障

公司拟使用非公开发行股票募集资金建设安全升级项目。2016 年，经中国证券监督管理委员会证监许可[2016]129 号文《关于核准网宿科技股份有限公司非公开发行股票的批复》核准，公司向特定投资者非公开发行人民币普通股（A 股）股票 81,218,421 股，募集资金净额为 354,712.88 万元。以上募集资金到位情况已经瑞华会计师事务所（特殊普通合伙）审验并出具瑞华验字[2016]48260004 号《验资报告》。

截至目前，募集资金投资项目云安全项目、海外 CDN 项目、面向边缘计算的支撑平台项目以及计算能力共享平台项目均已建设完毕并结项。截至 2022 年 12 月 31 日，公司募投项目节余及前次变更用途尚未安排使用的募集资金合计 125,896.20 万元（含银行利息及现金管理收益）。本项目的投入使用部分募投项目节余及前次变更用途尚未安排使用的募集资金。

另外，公司财务状况良好。2021 年，公司实现营业收入 457,501.47 万元；实现营业利润 17,301.06 万元；实现归属于上市公司股东的净利润 16,524.07 万元。公司拥有健康的现金流，为技术研发、项目建设及业务开拓奠定良好的基础。

第四章 项目投资、成果、效益分析

一、总投资情况

安全升级项目使用募集资金投入 21,000 万元，主要用于研发投入、设备采购、资源租赁等。

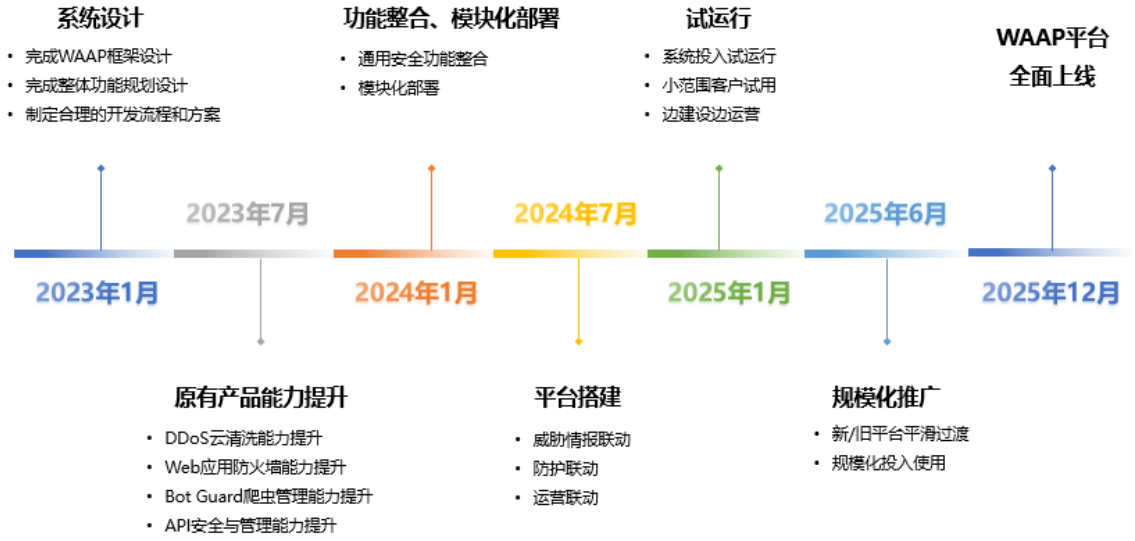
其中，使用项目建设募集资金 300 万美元（按照 2023 年 1 月 13 日汇率，折合人民币 2,018.76 万元）增资全资子公司香港网宿，并由香港网宿以同等金额增资其全资子公司香

港申嘉，由香港申嘉承担项目海外部分的建设。另外，使用项目建设募集资金 4,500 万元向全资子公司厦门网宿提供借款，由厦门网宿承担部分研发职能。剩余部分项目投入资金由公司作为实施主体。

二、项目实施周期和进度

本项目实施周期为 3 年，项目周期自 2023 年 1 月至 2025 年 12 月。

项目建设第一年，完成系统设计及原有产品能力的提升；项目建设第二年，完成通用安全功能整合及模块化部署，并完成威胁情报联动、防护联动、运营联动平台搭建；项目建设



第三年，系统投入试运行，边建设边运营，实现 WAAP 平台全面上线规模化使用。

三、项目成果

本项目主要研发成果具体如下：

1、安全底座夯实。DDoS 云清洗、Web 应用防火墙、Bot Guard 爬虫管理、API 安全与管理等产品自身能力提升，为 WAAP 整合方案夯实底座。包括：

（1）DDoS 云清洗场景化防护性能提升

（2）Web 防护策略优化与管理

（3）Bot AI 防护与动态对抗

（4）基于业务与数据视角的 API 安全治理平台建设

2、打造智能化的 AI 防护模型。将多年攻防基因及多行业客户运营经验注入 AI 模型，打造智能、自适应、持续进化的 AI 防护模型。

3、实现安全策略模块化。Web 应用与 API 安全策略梳理、整合、实现模块化配置。

（1）一键接入、高效防护。客户通过 WAAP 平台实现 Web 应用与 API 业务的一键接入，大大降低安全运营成本；

（2）统一管理，便捷运维。通过 WAAP 平台统一管理的能力，实现业务全局防护，在统一的管理平台进行安全策略的集约化管理；

（3）即开即用，按需开启。客户可按需自助开启所需的功能模块，降低防护成本。

4、情报联动。基于网宿平台海量攻防样本，优化数据清洗与关联分析能力，实现威胁情报的场景化适配和精准度提升。

5、防护联动。基于统一的 WAAP 平台，实现安全防护模块联动防护，全面封堵各类网络攻击。

6、安全运营赋能。基于网宿安全运营专家在各个行业的多年攻防经验积累，将安全运营经验以模板的方式开放给客户，实现安全运营赋能。

7、安全大脑建设。通过平台级数据联动，完善威胁分析能力，更好地捕获潜在的攻击威胁。

四、效益分析

本项目是对公司现有云安全平台及产品进行的升级研发，研发升级后产品实现的效益是公司对该产品历史累计投入的结果，无法单独核算因本次募集资金使用而产生的效益。根据公司技术积累以及行业发展趋势，预期本项目实施后，将对公司收入、利润产生积极影响。

五、项目涉及的审批事项

1、本项目的土地落实情况

本项目在公司现有办公场地实施，不涉及土地、房产购置事项。

2、项目的环保审批情况

本项目为软件研发类项目，非生产型项目，不产生废气、废水、固体废弃物等污染物。

第五章 项目建设风险

1、技术风险：如果在本项目实施过程中关键技术难点没有突破或者没有达到预定效果，将会对项目建设造成不利影响；另外，公司的竞争力是核心技术，如果项目核心技术人员流失，将可能导致项目核心技术流失或泄密，给项目造成重大影响。

2、市场风险：项目发展受到行业政策、市场竞争、市场需求等因素影响，如市场情况发生重大变化，将给项目业务拓展带来影响。

公司将继续在研发方面加大人力、物力投入，确保本项目的顺利实施。同时，公司将跟踪市场情况、和客户保持紧密沟通，及时了解市场动向，从而打造更符合市场需求、更有竞争力的产品及服务。

第六章 结论

本项目在公司原有安全平台及安全产品上进行升级、改进，项目的实施符合公司的战略布局，能增强公司在安全市场的竞争力，为安全业务开拓提供持续动力。

公司已对本项目进行了充分调研和准备，从技术层面来看，技术路径具有一定的先进性和相当的可行性；从市场需求来看，存在投入的必要性。

网宿科技股份有限公司 董事会

2023 年 1 月 13 日