INESA 上海仪电 | 上海南洋万邦软件技术有限公司
Shanghai Nanyang Wanbang Software Technology Co.,Ltd

安全运营服务

上海南洋万邦软件技术有限公司

1 南洋万邦公司介绍

上海南洋万邦软件技术有限公司
Shanghai Nanyang Wanbang Software Technology Co.,Ltd

上海南洋万邦软件技术有限公司

我们的愿景

让用户的信息系统更有价值

立志成为“国内领先的新一代信息技术服务提供商”，以企业及政府为中心，让数据增值，为城市赋能，助力用户数字化转型。

南洋万邦

成立于1992年，现隶属上海市属国有大型企业集团——上海仪电集团

云赛智联（股票代码600602/900901）全资子公司

上海软件和信息服务业百强、科技小巨人、高新技术企业

业务定位：以云计算、大数据为基础的新一代信息技术服务提供商

公司概况

上海（总部）
Shanghai

地址：上海市宜州路180号华鑫天地B6栋2-5楼
总机：021-52199000
邮箱：nywbmarketing@nysoftland.com.cn

2022年南洋万邦销售收入达到16亿+元

8家 子公司

分别设在上海、苏州、广州、香港特别行政区

650名 员工

其中技术人员400+人

2.6万 政企客户

分布全国30个省市自治区

100+ 国际国内IT知名厂商合作伙伴

2022-2023大数据产业领军企业
2022年度上海市优质大数据服务供应商
2020中国数字化最具影响力企业
2019年中国最具影响力软件和信息服务企业

南洋万邦与微软

微软中国重要合作伙伴

4次获得微软全球Country Partner of the Year

南洋万邦依托于母公司上海仪电和云赛智联定位智慧城市建设领军者及自身30年的雄厚IT技术实力，紧随云计算、大数据、智能物联等领域的快速发展。

南洋万邦打造了南洋云管平台一站式“云托管”综合解决方案和技术服务

全面支持微软Azure/M365/D365/Power Platform。

AE MSP　Security Service Partner　Gold Data Platform

Azure Migration Partner　Gold DevOps

Gold Microsoft Partner Azure Expert MSP Microsoft

Azure IOT Solution Aggregator

Fast Track Partner Gold Data Analytics

D365 CSA Partner　Gold Message

Gold Datacenter　Gold Collaboration and Content

南洋万邦发展历程

31年

高速发展，智动未来！

政企数据建运一体化总集成商和总运营商

1992年

由三名上海交通大学毕业的大学生联合创立：上海南洋微电子有限公司

1993年

成为微软公司在中国第一批授权代理商

1996年

成为SYMANTEC、VERITAS、AUTODESK等国际著名软件厂家的核心代理商

2003年

成立南洋苏州子公司

南洋万邦

2007年

公司更名“上海南洋万邦软件技术有限公司”

2013年

加入仪电集团

INESA 雲賽 上海仪电

2015年

成为上海仪电集团旗下“云赛智联股份有限公司” 全资子公司

INESA 云赛智联

2020年

合资成立南洋宏优、南洋道客两个子公司

共计拥有3个全资子公司，5个控股子公司

Gold Microsoft Partner Azure Expert MSP

——至今

- IT咨询规划
- 信息系统设计实施
- 技术支持
- IT运维外包
- IT培训认证

业务资质&标准认证

- 增值电信业务许可（信息服务业务）
- 信息系统建设和服务能力（三级）
- 电子与智能化工程专业承包资质（二级）
- 信息安全风险评估（三级）
- 信息系统安全集成（三级）
- 信息系统安全运维（三级）
- ISO9001-质量管理体系
- ISO20000-IT服务管理体系
- ISO27001-信息安全管理体系
- 信息技术服务标准（ITSS）运维能力成熟度（三级）
- ISO22301-业务连续性管理体系
- ……

合作厂商&市场地位

微软金牌能力合作伙伴，微软全球Azure Expert MSP

华为金牌合作伙伴，首批华为云授权支持中心，三钻认证服务商

Adobe、Veritas白金级合作伙伴，市场份额全国第一

浪潮钻石增值合作伙伴

VMware、Dell、爱数、亚信安全白金合作伙伴

Citrix、EMC、Nutanix、Oracle、Fortinet、Veeam、深信服、绿盟、天空卫士、联软金牌合作伙伴

微软FY14、FY17、FY18、FY22
全球Country Partner of the year

微软FY20最佳CSP合作伙伴
最佳Solution Aggregation合作伙伴、

Adobe年度最佳合作伙伴、最佳区域销售、最佳产品经理

华为价值
合作伙伴奖

Veritas大中华区最佳合作伙、
最佳BE业务渠道合作伙伴

VMwareF最佳区域合作伙伴、最佳
区域贡献奖

荣誉&奖项

所获政府、集团荣誉

上海市第十八届、十九届、二十届文明单位

2012-2014、2015-2016、2017-2018、2019-2020仪电系统先进基层党组织

2015-2016、2017-2018、2019-2020云赛智联系统先进基层党组织

2022上海市国资委100个党建工作品牌——“随申码”保障党员突击队

2022年上海市青年五四奖章集体

2022年度上海市优质大数据服务供应商

2021上海市三八红旗集体

2021上海市国资委系统青年突击队——上海市大数据中心青年突击队

2019上海市和谐劳动关系达标企业

2019上海市巾帼文明岗

2018年上海市五一劳动奖状

2017年上海市总工会模范职工之家

2016年上海市青年五四奖章集体

2016年上海市国资系统先进基层党组织

所获行业荣誉

2018-2022五次蝉联上海市软件和信息技术服务业百强

2022-2023大数据产业领军企业

2022年数字化转型领航企业

2021年度中国大数据技术应用领军企业

2021-2022数据商业领域领军企业

2020中国数字政府领军企业奖

2020中国数字化最具影响力企业

2019年中国最具影响力软件和信息服务企业

2019中国信息安全优秀服务商

2019年、2020年上海市高新技术成果转化百佳

2018中国软件行业最具影响力企业

2018中国互联网大会云计算管理服务领军企业奖

2017年全球物联网峰会杰出产品奖（IOT）

上海市合同信用等级AAA级企业/上海市守合同重信用企业

行业合作伙伴

国际一流的合作伙伴

公有云	Microsoft 阿里云 aliyun.com HUAWEI 天翼云
私有云	HUAWEI vmware SANGFOR 深信服科技
信息安全	VERITAS paloalto NETWORKS Symantec EISOO 爱数 FORTINET AsiaInfo 亚信安全
人工智能	Microsoft 阿里云 aliyun.com 腾讯云
大数据	Informatica Microsoft ORACLE

2 核心能力及解决方案

南洋万邦安全服务体系

建立以风险管理为核心的一体化安全服务

安全标准及合规性指导集成实施
安全运营流程指导安全集成业务

安全体系建设

目标一
提高用户安全管理水平

通过安全体系建设，能够有效的提高信息安全方面的技术及管理水平，通过等级保护安全测评。

安全整改加固

目标二
提高用户安全防御能力

通过国家安全标准的要求，对现有脆弱性、威胁性、缺失项进行安全整改与安全加固，提升安全管控及防御能力。

国家安全标准

信息中心

业务安全连续

社会影响

各安全厂商
安全技术驱动

收益一 **业务得到保障，规避风险**

通过信息安全的管控及防御措施的建设，对自身业务的风险降低。

收益二 **业务安全得到提升，提高效率**

通过安全集成支持业务流程安全且顺畅，让业务安全请求得到满足。

收益三 **业务安全得到改进，降低风险**

较好的安全管理体系，可以让业务数据安全可靠，不被篡改与窃取，更对业务安全连续提供可靠保障。

安全规划咨询

安全集成

业务、数据安全服务

等级保护

南洋万邦通过**中国网络安全审查技术与认证中心颁发的信息安全服务资质三级认证**，包括信息系统安全集成、安全评估、安全运维三个方向。安全服务团队按照信息系统建设的安全需求，采用信息系统安全工程的方法和理论，将安全单元、产品部件进行集成。对客户方所属的计算机信息系统的安全性、可靠性从技术层面和管理规范层面进行检查、评价、加固、保护等活动。并提供全过程、全生命周期地安全保障。

南洋运维服务能力概览

专职运维团队

7X24运维中心

原厂联合支持

工程师数据量

120+

高级工程师：**45%**

服务交付经理：**20%**

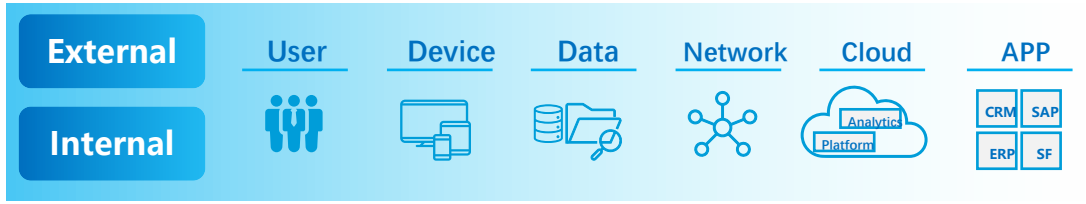
年度增长率：**35%**

自动化运维工具

自动化迁移工具

全国交付能力

南洋万邦安全解决方案



设备管理

- 设备磁盘加密（BitLocker）
- 终端管理（SCCM）
- 移动设备管理 (Intune)
- 终端威胁防护（MDE）
- 生物指纹（Win Hello）
- ……

数据管理

- 终端数据安全（MIP）
- 数据防丢失保护（DLP）
- 邮件数据安全 （MDO）
- 风险标识保护（AADIP）
- 客户密码箱（Customer Lockbox）
- ……

访问管理

- 高级威胁保护（MDI）
- 多因子身份验证（MFA）
- 混合身份验证（HMA）
- 特权访问控制（PAM）
- AI威胁防护（Azure Sentinel）
- 混合云安全（Azure Defender）
- 远程访问保护（Azure Bastion）
- 分布式拒绝服务 (DDoS)

应用管理

- 云应用安全及合规（MCAS）
- 单点登录（AAD SSO）
- 应用程序防火墙 (WAF)
- 安全Web应用（AFD）
- 密钥保管库（AKV）
- ……

咨询

解决方案

创造价值

现代化终端安全

组织需要跨移动设备、桌面设备和虚拟端点来管理和启用对企业资源的安全访问。我们通过结合微软产品来加强端点的防护，并且能够帮助企业降低安全风险。

涉及产品：Intune、CM、MDE

数据安全治理

通过扫描工具来对混合环境中的数据进行扫描机分类，通过自定义的标签来对数据、用户进行分权、分级，结合DLP技术方式数据的无意外泄。

涉及产品：MIP、AIP Scanner、PP、Endpoint DLP

身份安全防护

身份作为组织中最关键的核心，是基础设施的基石，通过身份监控、账户体系流程管控、多因子身份验证，单一登录等模块，为用户的整体身份安全提供保障。

涉及产品：MDI、Azure AD、PAM、SSO

邮件安全防护

电子邮件是互联网应用最广的服务，网络钓鱼邮件是当今勒索软件载体及数据外泄，攻击入侵公司内部的最佳媒介。由此可见员工的邮件安全意识对公司维持有效安全 防御尤其关键。

涉及产品：MDE、MDI、MDO

企业安全运营

众多客户因对安全产品不熟悉，而无法更好的发挥微软产品价值，因此希望通过安全运营服务帮助客户解读环境问题，规划安全线路，做到全方位的防护

涉及产品：MDE、MDI、MDO、MCAS、Sentinel

Landing zone

Azure着陆区从规模、安全治理、网络和身份考虑。帮助客户在 Azure 中实现企业规模的应用程序迁移、现代化和创新。

涉及产品：Azure Backup、MDC、VPN、Firewall...

MLPS on Azure

通过南洋专业的安全团队帮助企业完成Azure云上业务的等保安全认证，极大提升了企业关键业务的安全防护能力。

涉及产品：Firewall、Azure安全中心、WAF、NSG、Network Watcher

云安全评估

通过评估客户Azure的安全基线，帮助识别客户在Azure中应用的安全问题，并根据评估的相关信息结合等保要求对客户Azure租户提供Azure安全的整体配置评估及后续优化建议。

涉及产品：Azure安全中心、WAF、NSG、Network Watcher + Azure Policy

背景需求

日益复杂的安全威胁风险引发智能安全运营平台的需求

威胁攻击手段趋于组织化
静态防御手段无法应对

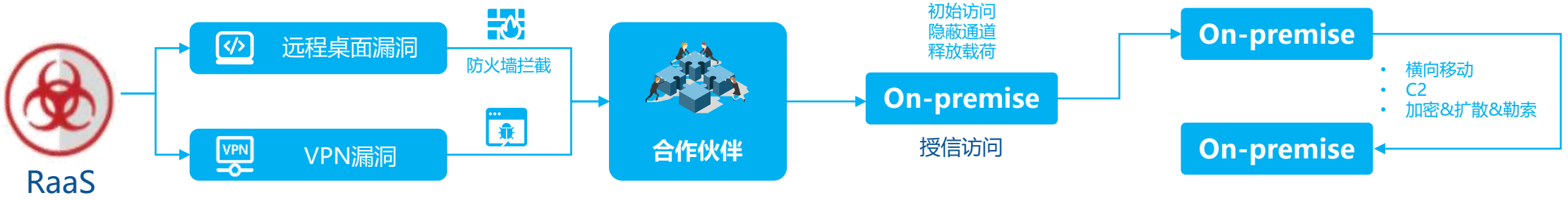
- APT等高级威胁难检测
- 0day等未知漏洞难发现
- 异常网络操作行为难检测
- 新型恶意程序等难以检测

组织业务不断变化
原有防护出现疏漏

- 新业务、新技术带来新威胁
- 无法及时掌握资产变化情况
- 漏洞检测、处置是否全面
- 资产、漏洞、威胁、事件

安全设备各自为战
策略无法有效执行

- 安全各自为战，不能形成合力
- 安全策略有效性难验证难优化
- 各类安全产品形成信息孤岛
- 缺乏联动响应能力



安全运营解决方案

提供威胁管理的全面功能

安全运营中心 （SOC） 是集中式的安全管理模式，它集成了人员、流程和技术，能够发现潜在的网络安全威胁并提醒企业。 建立 SOC 可以改善企业的安全状况，同时预防、检测、分析和响应网络安全事件。

南洋的 SOC 解决方案关键能力

架构和部署

包括单一部署、分布式部署、云部署等，包括与 SIEM 解决方案高度互补的自有或第三方解决方案的集成，以及客户自己的方案需要集成到SIEM中。

数据收集与优化

结构化和非结构化数据采集、范化、安全传输、安全存储。

事件溯源

威胁检测与分析、合规分析，包括用户异常行为分析、ATT&CK映射、机器学习、主动狩猎等。

事件应对

快速、正确和有效地对事件进行分类、记录和管理。快速创建安全事件、案例、工单，并结合案例的完整上下文，加速事件管理和解决。

自动化

针对安全问题，设计相应情报源的自动响应，帮助IT团队快速缓解威胁。

流程化

报告以及安全操作、事件处置流程步骤 SOP 。

安全运营技术

01
使用ATT&CK框架自评安全能力

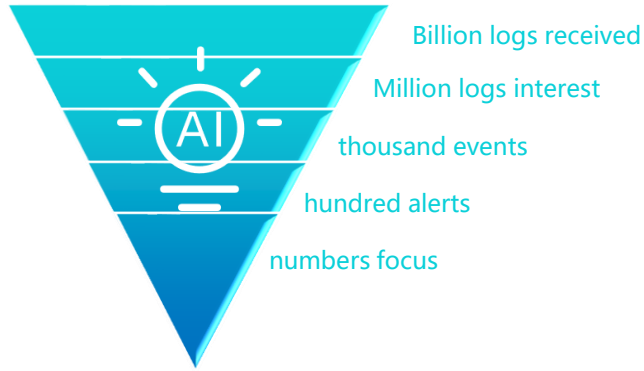
除了威胁建模以外，该框架大多用于识别当前部署的安全产品或工具中的风险处置能力差距，指导安全策略的实现，并评估采用新技术(如云服务)应对相关风险的可能。

02
调查来自所有数据源的威胁

保持事件的可见性，并将来自网络、端点和云环境等的异构安全事件关联起来进行分析，是成功检测和预防威胁的关键步骤。

03
AI与自动化

全面的威胁模型，海量事件的关联分析，意味着自动化成为必然。让攻防成为一场均衡的较量。·



安全运营平台演进规划

安全合规平台

安全事件管理能力

安全运营管理赋能

智能安全运营管理

安全合规平台

- 建立统一安全管理界面
- 完成安全事件系统对接
- 具备安全规则管理体系
- 实现安全事件标准化
- **AI智能风险监管模型**

安全事件管理平台

- 具备领导视角安全态势分析
- 完善优化安全事件规则场景
- 建立安全告警事件响应机制
- 结合情报提高安全分析水平
- **海量安全告警事件智能收敛**

企业安全运营中心

- “技术+人+流程”体系化运营
- 实现业务风险评估及处置机制
- 形成统一信息安全共享知识库
- 实现企业安全事件运营KPI目标
- **智能资产风险量化模型辅助决策**

智能安全运营中心

- 加强安全事件与业务风险融合
- 避免因安全事件导致业务中断
- 实现业务系统防欺诈体系
- 防止因业务风险造成名誉损失
- 防止因安全事件引发企业舆情
- **借助AI形成智能安全运营中心**

AI助力的全新SOC在传统安全运营中心功能的稳固基础上，凸显了更多的检测识别和响应能力。

南洋万邦运维保障服务中心

安全运营平台定位&价值

智能安全运营管理平台

以企业业务为核心，通过流程覆盖、技术保障及服务化，构建集识别、防护、检测、响应于一体的全面安全体系。

首次将AIOPS理念注入企业安全运营实践中，通过将传统安全事件分析能力与机器学习，人工智能技术相结合，形成智能安全态势感知、威胁情报调查、智能合规监测、智能安全审计等 信息安全运营闭环场景，实现安全运营向运营智能化的方向持续演进。

客户案例

安全运营

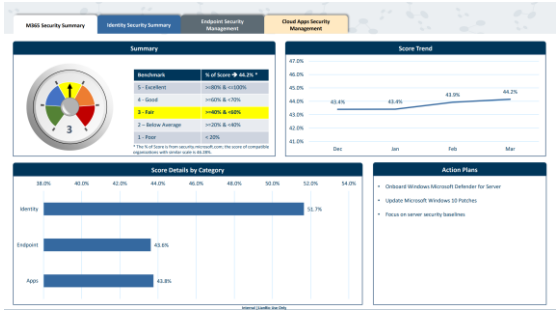
该客户是一家处于临床阶段的生物制药公司，专注于利用人工智能平台为自身免疫疾研发新型治疗药物。随企业发展越来越多的设备接入网络，现有管理模式无法实时了解全局安全事件，无法有效规避安全风险。

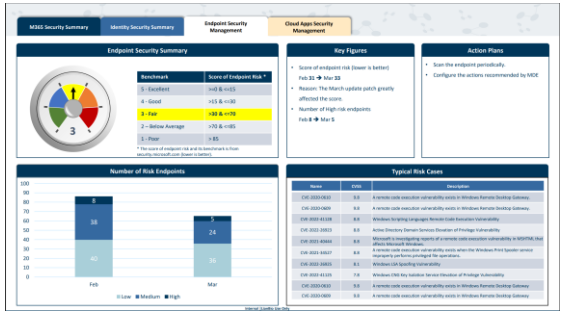
挑战 & 现状

- 大范围且不合规的移动设备的使用
- 无成体系的长效化安全预警机制
- 缺少专业的安全人员，安全事件处理缓慢
- 无法实现自动化安全运营及全局的有效管理
- 无安全时间应急响应流程及保障体系
- 当前安全组件过于分散，没有统一化的管理平台

价值 > 收益

- 为企业定义勒索病毒响应预案，在产生勒索病毒时，有效抵御。
- 终端管理方案+企业安全运营，极大的提升了用户保障。
- 持续性企业完善安全推进路线图，定期进行安全研讨会。
- 通过自动化运营流程，提升其工作效率，减少了安全人员投入。





INESA
上海仪电

上海南洋万邦软件技术有限公司
Shanghai Nanyang Wanbang Software Technology Co.,Ltd

谢谢！

上海南洋万邦软件技术有限公司
地址：上海市宜州路180号华鑫天地B6栋2-5楼
总机：021-52199000
邮箱：nywbmarketing@nysoftland.com.cn