数据安全成为业务加速器?

组织竞争力背后的无名英雄

中国洞察

联合出品方

IBM | 亚马逊云科技

主题专家

Clarke Rodgers

企业战略总监
亚马逊云科技全球
linkedin.com/in/clarkerodgers
rodgclar@amazon.com

Clarke 拥有 20 多年构建和管理网络安全计划的经验，目前担任亚马逊云科技企业战略总监。Clarke 致力于帮助客户高管探索如何利用强大的安全性、风险与合规性计划来推动业务发展和加速创新。Clarke 于 2016 年加入亚马逊云科技，为几乎所有行业（从金融服务、医疗保健、媒体和娱乐到政府）的 700 多家客户提供了数字化转型（人员、流程、组织变革）以及安全、风险、合规性和隐私方面的建议。作为一名美国海军陆战队退伍军人，Clarke 对于如何通过强大的安全计划创造业务成效拥有独特的见解。

Chris McCurdy

全球副总裁兼总经理，
IBM 安全服务
linkedin.com/in/chrismmccurdy
cmccurdy@us.ibm.com

在过去 15 年以来，Chris 曾担任多个领导职位，负责指导 IBM 安全服务的销售和战略，始终一如既往地推动安全业务的快速增长。在加入 IBM 之前，他曾在 Andersen、International Network Services 和 Lucent Technologies 等多家咨询公司担任管理顾问。他还在美国的一家大型零售汽车集团担任 CIO。Chris 拥有贝勒大学信息系统工商管理学士学位，并且是一名认证的信息系统审计师。

Gerald Parham

全球安全研究负责人兼 CIO，
IBM 商业价值研究院
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald 在 IBM 商业价值研究院负责领导安全和 CIO 研究领域。他致力于为高管和董事会成员提供技术与安全战略、网络风险和网络价值链方面的建议。Gerald 在高管领导、创新和知识产权开发领域拥有超过 20 年的经验。他拥有加州州立大学和南加州大学的科学和艺术高级学位，以及约翰霍普金斯大学的写作学士学位。

白帆

安全合规与治理服务总监
亚马逊云科技大中华区
johnxbai@amazon.com

白帆先生于 2021 年加入亚马逊云科技，负责亚马逊云科技安全、合规与治理产品在大中华区的战略。他负责推动亚马逊云安全、合规与治理产品在中国区域的落地与推广，帮助亚马逊云科技大中华区的用户满足全球合规要求，以及提升安全与合规体验。白帆先生在网络安全领域有超过 20 年的工作经历，包括在大中华以及亚太地区的研发、客户支持以及销售管理岗位。

王晓野

数据产品技术专家总监
亚马逊云科技大中华区
wangxy@amazon.com

王晓野先生负责带领亚马逊云科技大中华区数据领域专家团队提供云上架构方案设计及实践指导，同时致力于亚马逊云数据库，数据分析及机器学习服务在中国市场的应用和推广。他拥有多年留法工作经历，长期专注于企业分析及大数据能力建设。

摘要

安全、可信的数据有助于促进创新并建立竞争优势。

依靠强大的数据安全建立信任，释放业务价值。

最近的研究表明，高绩效型首席数据官在评估数据有效性时会将信任和安全性列为优先标准。

利用跨职能协作创造价值并增强数据安全。

数据和安全高管需要与运营和技术高管开展合作，以充分发挥数据的价值。

安全意识文化有助于改善业务成效。

安全意识必须从“守门人”转变为“业务赋能人”，从“说不”转变为“思考如何实现目标”。

释放信任的价值

在数字经济中，数据就是氧气，为创新赋予生命力。而保障数据安全对于组织建立信任和创造价值至关重要。事实上，根据 IBM 商业价值研究院 (IBM IBV) 的调研，具备最先进安全能力的组织在五年内的收入增长率要比其他组织高出 43%。[1]

然而，数据损坏或数据泄露可能会造成严重的业务损失。IBM Security 近期发布了《2022 年数据泄露成本报告》，报告揭示数据泄露事件给企业和组织造成的经济损失和影响力度达到前所未有的水平，单个数据泄露事件给来自全球的受访组织造成了平均高达 435 万美元的损失，创下该年度报告发布 17 年以来的最高纪录。[2] 如果数据信任受到破坏，则会阻碍业务增长并增加支出。

为应对这一挑战，最优秀组织的做法是基于可靠的安全数据快速建立信任，然后利用这些可信数据来创造机遇。在本报告中，我们甄别出了成功领导者在管理和保护数据方面的共同点，包括他们运用哪些范式、实践和优先要务来助力建立竞争优势。

洞悉未来

最近，IBM 商业价值研究院和亚马逊云科技针对超过 3,300 名 CDO（其中约 300 位来自中国），分别开展了独立研究。研究结果表明，最成功的首席数据官 (CDO) 将安全、可信的数据列为业务价值的关键驱动力。具体来说，利用可信数据作为业务加速器对于组织至关重要。

最成功的首席数据官将安全、可信的数据列为业务价值的关键驱动力。

在 IBM 商业价值研究院的调研中，CDO 将数据安全列为其最重要的责任。[3] 同样，在亚马逊云科技 CDO Agenda 研究报告中，受访的 CDO 均表示数据治理（数据安全的基本要素）是其首要任务。[4] 这些 CDO 首先会保障数据安全，以此与员工、客户和合作伙伴建立信任；然后，他们会利用这种信任关系来激活数据价值，并更加快速、信心十足地推动业务增长。

高绩效型 CDO 在数据安全举措上更进一步。IBM 商业价值研究院根据四个维度：建立从数据到价值的清晰路径；利用数据投资加速业务增长；数据是业务模式创新的核心要素；参与生态系统合作，从受访 CDO 中甄别出了一类脱颖而出的“数据价值创造型 CDO”，此类 CDO 只占全部受访 CDO 的 8%，还属于凤毛麟角。但是和全球平均水平相比，“数据价值创造型 CDO” 所在组织的创新能力高出 43%，数据资本化高出 9%，收入增长率高出 10%。而在中国，虽然“数据价值创造型 CDO”只占中国全部受访 CDO 的 6%，同样也是凤毛麟角，但是和全球平均水平相比，他们的创新能力高出 20%，数据资本化高出 15%，收入增长率则尤为出众——远远高出了 54%。[5] 而且，此类 CDO 在数据相关业务流程上分配的支出较少，但却实现了与其他 CDO 相当甚至更高的价值。

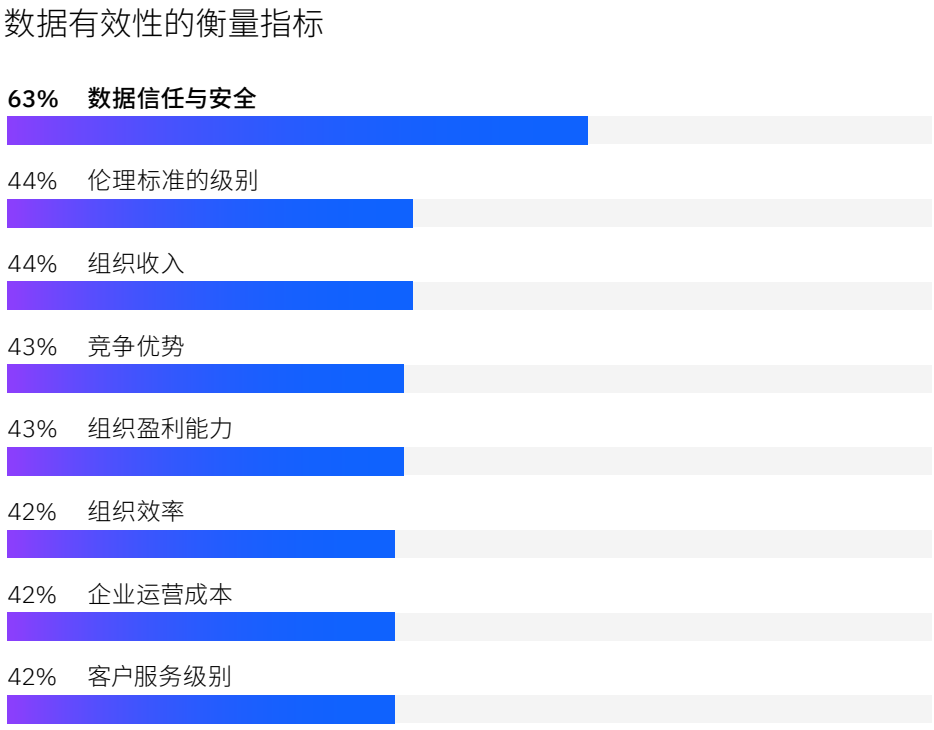
此类 CDO 具备一项关键的差异化特征 — 他们会采用独有方式将数据与安全、运营和技术战略相结合。他们更加注重网络安全、数据伦理、数据架构透明度以及建立对数据有效性的信任（见图 1）。

这些领先组织推动成效的实践可供任何其他组织效仿。正如这些领先组织所展示，如果以系统性和严谨的方式应用最基本的数据清理实践，组织将能够实现更高的数据敏捷性。而这又有助于推动以更明智的方式承担和管理风险，增强运营灵活性，并最终改善业务成效。接下来，本报告将提供一个切实可行的路线图，助力组织通过安全、可信的数据来建立竞争优势。

图 1

更加注重可信数据

领先的 CDO 基于信任和安全性来衡量数据有效性。



高绩效型 CDO 更加注重“数据信任与安全”，远远超出其他数据有效性衡量指标。

信息来源：“全球最高管理层系列 - 化数据为价值：卓越首席数据官事半功倍创造价值”，IBM 商业价值研究院。2023 年 5 月。

推动数据创新

前赛车手马里奥·安德雷蒂 (Mario Andretti) 曾说过：“令人惊讶的是，有许多赛车手，即使是一级方程式赛车手，也认为刹车是用来减速的。”其实恰恰相反，正如马里奥·安德雷蒂在职业生涯中所展示，刹车可以帮助经验丰富的赛车手开得更快。[6]

同样，强大的数据安全可以帮助组织建立信心，并更加高效地创造价值。如果企业确信已实施有效的安全控制，就可以敢于更迅速地采取行动并承担风险。

领先的 CDO 就成功展示了这一点。他们的组织运用现代技术工具来帮助保护数据免遭未经授权的访问，助力实施数据隐私，并有效管理合规性与治理。这些组织建立了一个安全基础来支持更快地实现运营目标，包括增加收入和利润、改善客户关系和营销、推出新产品和服务，以及优化流程、业务模式和战略。[7]

确保数据、运营、技术和安全策略与组织的主要业务目标（或“北极星”）相一致，最终有助于增强数据安全并建立所需信任以改善决策和绩效（见图 2）。企业领导者应当认识到各个职能领域之间的密切合作关系，并营造一种积极协作的环境，通过相互关联的职能战略来快速推动大规模创新。

领先的数据组织还认识到文化有助于驱动成效。他们采用不同的方式落实以下举措：

– 消除破坏信任的障碍

– 建立安全意识文化

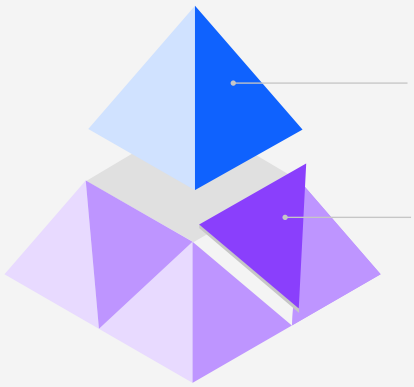
– 制定企业韧性规划

就像赛车中的刹车一样，强大的数据安全可以帮助组织建立信心并更迅速地采取行动。

图 2

高绩效的秘诀

数据和安全是整体价值引擎中的
两个组成要素。

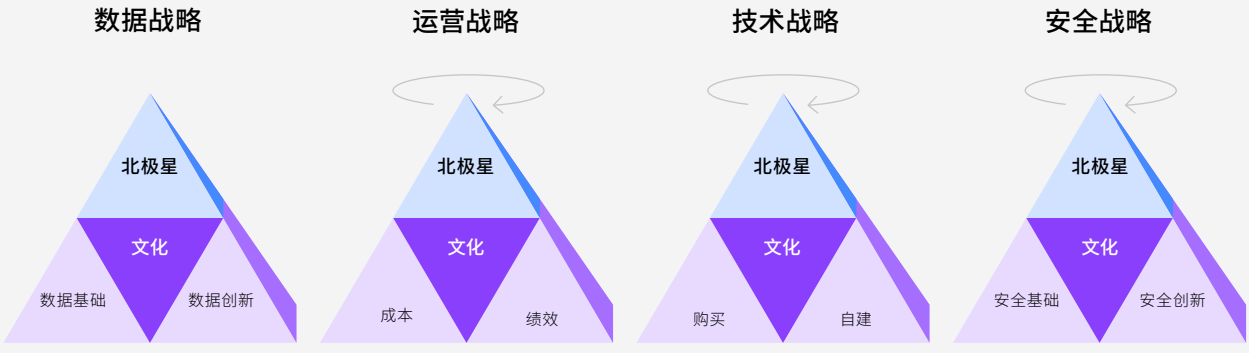


价值引擎

北极星
在业务战略中融合价值（增长）与价值观（使命）

文化是将不同领域的战略联系在一起的纽带

- 核心价值观：诚信、透明地行事
- 沟通：提高意识并建立信任
- 协作：推动洞察和创新
- 协同：增强韧性并扩大范围



A 面　B 面　C 面　D 面

信息来源：IBM 商业价值研究院

领先实践一

消除破坏信任的障碍

改善组织的数据安全状况通常需要变革，而变革不可避免会遇到障碍，比如各职能采用孤立的专有解决方案，缺乏透明度和责任落实等。不过，通过有意识地应对这些挑战，组织可以增强数据安全，从而加速创造新的商机。

打通战略孤岛

营造一种安全、数据驱动的敏捷文化，利用数字环境与服务重塑传统业务，这句话说起来很容易，但是大多数组织来说都是一项艰巨的挑战。例如，数据、运营、技术和安全职能通常独立运作，并且分别采用不同的专有战略，而无法相互形成协同。为了通过运营效率或卓越绩效释放价值，这些不同的能力必须相互支持，并与组织的“北极星”相一致。“北极星”就是组织共同的业务战略和核心使命。

在亚马逊云科技 CDO Agenda 研究报告中，近三分之一的受访者表示，他们与其他最高管理层领导者共同承担数据管理的责任。[8] 这可能会被视为一项障碍，但企业领导团队认识到，他们需要通力合作才能取得成功，并通过合作关系建立更强大、更成熟的能力。如果未建立一种协作文化，让各职能领域的战略相互支持，组织将难以权衡多方需求，也无法就其最紧迫的业务需求达成一致。

企业领导者认识到整个组织内的协作和战略协同有助于建立信任。

减少运营摩擦

数字经济创造价值的核心在于数据的自由流动。随着集中式的静态数据让位于云端数据、本地数据、边缘数据和来自业务合作伙伴的数据，传统的安全策略和控制必须持续迭代以应对日益增长的复杂性的风险。企业领导者深知，他们的企业必须要超越网络边界和托管基础设施，关注数据本身，对静态数据、动态数据和使用中的数据进行加密。

展望未来，同态加密、区块链、AI 生成的内容和自动化决策将对长期以来的数据安全实践和假设构成挑战。[9] 因为新技术会进一步增加现有安全策略和控制方法的复杂性。企业领导者必须关注未来趋势，采用如零信任以及权限管理等工具及策略，并将其纳入数据企业数据管理机制。

消除模糊性

无论对于内部业务用户还是外部客户，透明化数据访问、存储、处理和共享方式都是至关重要的，尤其是在高度监管的行业中（参见“观点：建立信任”）。然而，过去的数据管理实践和数据架构通常无法提供对组织所使用的各种海量数据的可见性。IBM 商业价值研究院的最新研究和亚马逊云科技之前的研究都表明，了解源数据的团队与使用该数据做出决策的一线用户之间需要更高的透明度。[10]

CDO 意识到必须缩小这种透明度差距，否则数据信任度就会下降，尤其是在最高管理层中。根据 IBM 商业价值研究院的调研，68% 的受访 CDO 表示其组织的员工在很大程度上信任组织的数据，但近 40% 受访 CDO 表示其最高管理层团队并不信任组织的数据。[11] 这可能反映了对数据分类、数据安全和数据治理的潜在担忧。CDO 必须采用自动化工具，发现、管理以及处置敏感数据，消除这种怀疑，否则这将削弱投资、发展动力和业务潜力。

观点

在高度监管的行业中建立信任：机会就在眼前

随着我国《数据安全法》《网络安全法》《个人信息保护法》等法律法规的陆续出台，每一个组织都必须满足最低的数据安全基线才能信心十足地开展业务。而在处理敏感数据的高度监管行业中，数据安全基线更高。例如，在健康医疗行业，国家卫健委于 2018 年 9 月发布的《国家健康医疗大数据标准、安全和服务管理办法(试行)》，对县级以上卫生健康行政部门(含中医药主管部门)、各级各类医疗卫生机构、相关单位及个人所涉及的健康医疗大数据进行全面监管。在工业及信息行业，工业与信息化部于 2023 年 1 月 1 日正式实施的《工业和信息化领域数据安全管理办法》（试行），对在中华人民共和国境内开展的工业和信息化领域的数据处理活动及其安全进行监管。在金融行业，为规范中国人民银行业务领域数据的安全管理，中国人民银行于 2023 年 7 月发布《中国人民银行业务领域数据安全管理办法(征求意见稿)》。在医疗保健、银行和金融服务、能源和制药等行业中，四分之一的数据泄露成本是在数据泄露发生两年多后才产生的。[12] 这些成本包括长期以来的监管和法律成本，以及因个人敏感信息和个人身份信息 (PII) 泄露而产生的品牌声誉损失。[13]

2023 年第一季度，涉及我国的数据泄露事件仍呈现高发态势，受影响较大的行业包括教育、卫健、金融等。其中，单次遭泄露数据量在 10 万至 100 万条区间内占比最高，接近总量的一半，而遭泄露数据仍以公民个人信息为主，占比 71%，系统业务数据和企业信息数据分别为 18% 和 11%。[14]

在高度监管的行业中，CDO 最大的一块短板（也是最大的商机）就是未将安全数据成效视为优先要务。根据 IBM 商业价值研究院的调研，只有 30% 的银行和金融市场 CDO 可能会将数据监管合规性视为一项关键责任。值得注意的是，只有约一半的银行和金融市场 CDO 表示遵守行业隐私和伦理政策及法规非常重要。[15]

我们在其他高度监管的行业也发现了同样的规律。只有 63% 的医疗保健和生命科学 CDO 和 63% 的政府 CDO 将行业隐私和伦理政策及法规视为优先要务。[16] 如果信任是一种来之不易而又容易失去的宝贵资源，那么解决数据隐私和伦理问题对于增强客户互动一致性、改善关系以及最终建立竞争优势至关重要。

案例

快递行业领先企业：统一的安全控制中心，集成无数“安全孤岛”

国内某规模型快递企业拥有覆盖全国 31 个省、自治区和直辖市的服务网络，超过 20 多万快递员，业务流转环节众多；企业内部还有很多不同的防火墙和终端；网点密集、设备多，对每个业务环节都做好数据安全管控极其重要。

该企业携手 IBM，建立起统一的安全控制中心，将无数“安全孤岛”进行集成。对于 IBM 的助力，该企业数据安全相关负责人是这样评价的，“借助 IBM 的安全解决方案，我们处理业务数据的效率大大提高。以更少的投入，更专业的运营，实现了大数据服务于业务的发展，完成了更多的工作，因此可以解放我们的安全人员，去做更有价值的事情。”

智能驾驶行业知名企业：全局数据架构，降低数据管理复杂度

中国智能驾驶应用和 AIoT 领域某知名企业在 AI 模型训练中所累积的数据量超过数十 PB，并且每年以若干 PB 的增量高速增长，这些数据分散在多中心、多云环境里，最初的基础架构面临着竖井林立、存取性能下降、数据调度困难、管理复杂、数据存放成本高等难题。

IBM 利用 Spectrum Scale 为该企业打造了全局平台，通过单一事实来源和全局数据架构，解决了复杂的数据系统问题。通过 Spectrum Scale统一了数据平台，企业不用再担心数据运维管理问题，在降低管理难度的同时提升了数据安全性。Spectrum Scale 可以统一管理磁盘和磁带，一方面，通过灵活的冷热分层策略帮助地平线每年节省数千万的存储成本；另一方面，高效的分布式数据存储管理也使得上层的数据管理中台与前台业务无需关心存储本身，从而更加专注于业务系统的研发与优化。

领创集团：全球金融服务解决方案，实现安全合规与业务稳定双保障

伴随东南亚人工智能 (AI) 产业的兴起，与之共同成长起来的一批科技企业由此进入了全球视野，2016年成立于新加坡的领创集团便是其中之一，旗下企业和消费者业务共服务超过 700 家企业客户、20 万家商户和 4000 万消费者。

增长之路需要强有力的技术底座。首先，系统稳定性至关重要，作为立足全球的金融公司，领创集团在海外扩张的进程中，拥有稳定、灵活、高可用的基础设施至关重要。此外，领创的业务场景复杂多样。例如，领创集团旗下消费者业务 Atome Financial 为东南亚用户提供 “先享后付” (Buy Now, Pay Later) 的时尚消费解决方案和数字金融服务，在与新加坡亚马逊电商等其他公司合作时，每逢的大型促销活动例如每年的双日，瞬时流量突增，就需要面对大流量和高并发的场景。而在领创处理 Atome Financial 的数字信贷业务时，还需要分析数据量庞大的用户支付数据，进行深入的消费行为分析，并实时监控风险。最后，在人工智能方向上，领创集团始终在积极探索，希望借助云上的算力资源降低机器学习的门槛，迭代风控模型等。

为了应对这些挑战，领创选择了亚马逊云科技。在短短 2 个月内，领创便在亚马逊云科技上成功构建了跨区域的业务容灾系统，大幅增强了其业务稳定性和抗风险能力。在高峰期，得益于亚马逊云科技的弹性计算，领创成功应对了高达平时流量 20 倍的瞬时峰值流量，满足了 Atome Financial 在电商促销时的业务需求，无需预置大量资源。2022 年和 2023 年领创在亚马逊云科技上的服务可用性已超过了 99.99%，且整体故障时间在 10 分钟以内。同时，利用机器学习服务，领创显著提高了 ADVANCE.AI 风控模型的响应速度，迅速应对新挑战，确保在风控行业保持领先地位并在全球金融领域稳健发展。得益于亚马逊云科技灵活、稳健的云基础设施，领创集团整体提升了业务可用性，实现了技术上的创新升级，为未来的全球业务扩张打下了坚实基础。

Source: 亚马逊云科技案例研究“亚马逊云科技助力领创集团打造全球金融服务解决方案，实现安全合规与业务稳定双保障“。2023 年。https://aws.amazon.com/cn/solutions/case-studies/advancegroup/

车联网领军企业：车联网信息安全架构，增强数据可视化

电动化、网联化、智能化、共享化已成为汽车产业发展潮流和趋势，但随着智能网联汽车集成度、复杂性的增加，除传统的功能安全以外，复杂网络和数据分析技术的应用也带来了新的风险和挑战，汽车数据安全问题逐渐受到广泛关注。

2022年 3 月，由国家工业信息安全发展研究中心牵头编制的《智能网联汽车数据安全评估指南》团体标准正式公开征求意见。在此背景下，中国车联网某领军企业通过采用 IBM QRadar 构建更智能的车联网信息安全架构，有效保护并大大降低所有联网的车辆面临的安全威胁。据评估，QRadar 在数据接入、可视化展示、智能分析、报告导出等方面都达到了预期效果。QRadar 的高级威胁检测管理和风险预警，能够从大量的异常数据中发现宝贵的数据洞察，与该企业产品整合之后，可主动应对信息安全的挑战。

领先实践二

建立安全意识文化，改善成效

就像驾驶赛车时获得充足的安全信心一样，组织应当建立一种安全意识文化。在这种文化中，领导者、员工、合作伙伴和客户对自己所使用的数据充满信心，这样就有助于营造更加可预测、可信和高效的环境。不过，从一线员工到董事会的全体人员都必须承担起数据安全的责任。

关注“如何实现目标”

优秀的组织会鼓励用全新的方式来思考安全问题。组织应当从领导层自上而下提高对网络风险的认识。这是一项势在必行的举措，因为一项研究发现，95% 的网络安全问题都可以追溯到人为错误。[17] 领先的组织会为团队成员给予激励和权限，让他们将安全视为优先要务，甚至可以在安全功能未按预期运行时延迟交付产品。

如果将安全性视为支持业务成效的引擎，而不仅仅是一种政策执行，这种全新的思维方式更容易被接受和采纳。随着领导者成功将安全性的角色从“守门人”转变为“业务赋能人”。安全决策将更多地关注“如何实现目标”，而不是不假思索就直接说“不行” — 这是一种决定性的思维转变。

从一线员工到董事会的全体人员都必须承担起数据安全的责任。

采取全新的人才方法

《2022 年数据泄露成本报告》还揭示了全球安全人员配备不足的现状。62%的受访组织表示，由于现有人手无法满足其安全需求，他们的数据泄露平均成本比人员配备充足的组织高出了 55 万美元。这一发现进一步印证了在安全领域携手合作的重要性。[18] 重新思考安全团队的组成（包括与非技术人员合作）有助于建立更强大、更多元化的安全屏障。从本质上说，数据和安全性涉及跨职能协作，因此领先的组织意识到必须用全新的方式来应对熟悉的挑战。

例如，人力资源专业人员可以更好地理解黑客按小时或交付成果获取报酬的行为模式和激励机制。将安全人员和安全能力赋能到各个业务，让业务了解安全，并且拥有对业务相关安全问题的决策权。营销和传播专业人员可以就如何以最佳方式分享数据泄露消息提供相应指导。一些没有大学学位的人员可能会因兴趣而熟练掌握新兴技术，这也是正规教育所无法教授的技能。[18] 这种开放式人才方法可以引入全新的视角，并扩充人才库的技能和专业知识。

打造合规、注重隐私且符合伦理的业务运营方式

尽管一些业务用户将合规性视为障碍，但实际上，合规性对于实现数据隐私和数据伦理至关重要。全球的数据价值创造型 CDO 表示，他们实现了比全球平均水平更出色的数据伦理、透明度和网络安全性（见图 3）。他们展现了这些能力如何帮助组织建立竞争优势。大中华区受访 CDO 在透明度方面优于全球平均水平，在数据伦理方面处于全球平均水平，而在网络安全方面仍略低于全球平均水平。

例如，积极主动的合规方法有助于消除摩擦。在最近的播客中，亚马逊云科技安全保障高级经理 Samara Moore 鼓励安全团队与其他业务和技术团队建立密切的合作关系，共同处理运营和监管问题。她建议领导者将合规性视为设计的一部分，并将合规功能嵌入解决方案。[19]

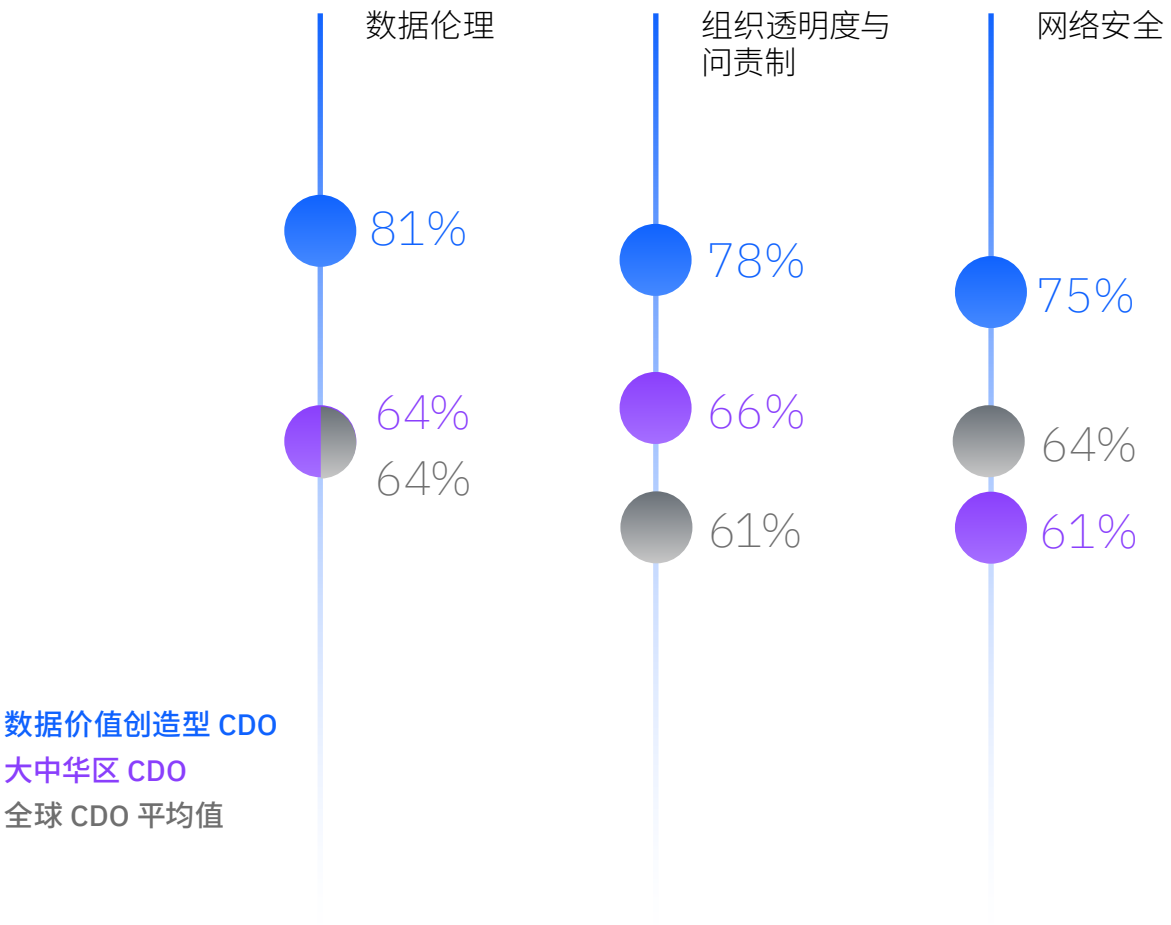
同样，合规管理软件有助于提高策略和控制管理的不可见性和自动化水平。研究表明，自动化合规工具可以将审计准备时间缩短高达 75% — 运营效率大幅提升。[20]

重新思考安全团队的组成（包括与非技术人员合作）有助于建立更强大、更多元化的安全屏障。

图 3

保护数据价值

“数据价值创造型”CDO 在与信任相关的数据实践方面优于其他 CDO。



信息来源：“全球最高管理层系列 - 化数据为价值：卓越首席数据官事半功倍创造价值”，IBM 商业价值研究院。2023 年 5 月。

OPPO: 数据安全是一切业务的基础

作为最早“走出去”的中国品牌之一，OPPO 能把业务拓展至全球，其过人之处不仅仅在于产品品质，而是着眼于用户的数据安全，构建相应的安全体系和措施，“重视安全合规”的理念已深深地融入到产品设计的全流程中。

为了更好地保护全球用户的数据安全，OPPO 希望获得健全、完善的数据安全与合规保护，在相应基础设施技术框架的帮助下，去满足不同国家与地区的安全合规要求。亚马逊云科技凭借优质的产品性能、与 OPPO 相一致的价值观脱颖而出。

高度安全、高度可用、弹性灵活的 Amazon CloudHSM 服务，满足了 OPPO 在安全合规方面的高等级要求，能够全面保护用户的数据安全，为海量用户保驾护航。得益于亚马逊云科技全生命周期的数据安全服务，用户对 OPPO 产品和服务更加信任，为 OPPO 在更大范围内的业务拓展打下了坚实基础。OPPO 数据安全架构师周洁说：“OPPO 始终站在用户的角度发自内心地践行安全合规，而非因为法律的约束被迫去执行，这是我们的初心。”随着量子计算、联邦学习（FL）、安全多方计算（MPC）、可信执行环境（TEE）等技术的逐渐成熟与应用，OPPO 考虑与亚马逊云科技继续开展广泛而深入的合作，双方共同致力于增强云端安全通信中的安全保护，坚守安全合规的“初心”不变，为终端用户提供更好的数据安全保护体验。

信息来源：亚马逊云科技公众号“数据安全难保障？亚马逊云科技为 OPPO 海量用户数据保驾护航“。2023 年10月17日。https://mp.weixin.qq.com/s/RdKEA0pCE6FkLWC35QRSDQ

泡泡玛特：全球在线商城，低成本安全出海

北京泡泡玛特文化创意有限公司（以下简称“泡泡玛特”）在“成为全球领先潮流文化娱乐公司”愿景的驱动下，在国内取得优秀成绩后，又将目光投向了海外的全球化市场。他们在欧美、亚太等区域的多个国家开展了线下门店业务，因而在线商城业务也需要针对相应地区进行部署。泡泡玛特在深思熟虑后，决定选择更具挑战的自主建站模式，这意味着公司必须拿出一整套方案来支撑在线商城的搭建和后续运营。

首先，针对不同国家和地区的运营，如何让业务符合当地法律法规要求十分重要。亚马逊云科技所提供的服务均通过了包括 ISO 在内的多达 98 个安全标准和合规性认证，且存储客户数据的全部 117 项亚马逊云科技服务均具有加密此类数据的能力，满足几乎所有全球监管机构的合规性需求，用户可直接继承，可有效降低泡泡玛特的相关审计成本。

其次，泡泡玛特的业务性质，决定了数据库是一系列相关功能的核心前提。在产品调研阶段，亚马逊云科技的数据库服务整体性能相对于友商产品，领先幅度超过 30%，Amazon RDS for PostgreSQL 和 Amazon Aurora 低成本及完全托管、高可用性的特点，很好地作用于在线商城的电商交易及产品库存环节，保证了泡泡玛特在不改变既定技术架构的前提下，在线商城也能流畅运转。

最后，Amazon ElastiCache 在可扩展至每秒数亿次操作的同时保持微秒级响应时间，有效记录日志，让一切尽在掌握。由于 Amazon EKS 强大的易用性，泡泡玛特得以在相对更短的时间内完成了容器技术相关的学习和容器的实际部署，在这方面同样获得了 10% 人力成本和时间成本上的节约。

通过以更低成本完成全球在线商城的部署运作，泡泡玛特在扩张自身企业规模、实现更大效益的同时，对于广大希望以自主建站方式开拓更广阔市场的国内出海企业，不啻为良好的借鉴。

信息来源：亚马逊云科技案例研究：“赋能独立站出海，泡泡玛特智选亚马逊云科技实现文化‘破圈’”。https://aws.amazon.com/cn/solutions/case-studies/popmart/

TCL实业：合规与隐私，为全球化部署构筑安全基石

作为一家聚焦智能终端业务的公司，TCL实业近年来大力发展 AI x IoT 全屋智能家电产品，构建智能家居生态圈。然而，AI x IoT 全场景智能家居生态圈在更加智能化和为用户带来更多便利的同时，也带来了新的风险和挑战，而最大的威胁之一是来自云服务平台的安全威胁。

在安全设计方面，TCL实业携手亚马逊云科技采用分级策略，保证安全设计的可靠性。在安全测试方面，TCL实业在自主研发的基础上，采用亚马逊云科技的云安全漏洞检测系列工具，配合人工审计，对产品进行渗透和认证等措施。在及时反馈方面，TCL实业建立安全应急响应中心，由专人负责运营。此外，经过一系列评估，TCL实业采用Amazon Key Management Service来解决密钥安全性的问题，采用了Amazon Security Hub、Amazon Transit Gateway、Amazon GuardDuty、Amazon CloudWatch 等服务获得全方位隐私及合规保护。

TCL实业通过在云服务端采用 Amazon WAF 来防护攻击，从监测的数据上来看，一周内抵御了超过 13 万次的恶意请求、接近 10 万次的程序自动攻击，防御效果显著。目前，安全与合规已经成为 TCL 品牌差异化的重要部分，而亚马逊云科技的云安全是这种品牌差异化的重要助推力量。

信息来源：亚马逊云科技案例研究“TCL 实业“。2022。
https://aws.amazon.com/cn/solutions/case-studies/tcl-case-study/

领先实践三

制定企业韧性规划

从全球疫情、供应链中断、极端天气、乌克兰战争到不确定的经济形势，随着各种突发事件接踵而至，组织正在应对一系列冲击，这些冲击颠覆了计划中的假设和传统的风险缓解措施。[21]

运营环境开始变得充满不确定性，有时甚至是混沌。与此同时，威胁行为者正在设法利用各种新漏洞。为应对这一形势，领先的 CDO 团队及其安全领导者正在大力加强基本的安全健康措施，从而改善数据治理并提高运营韧性（请参见“观点：回归基础”）。

走出舒适区

由于不确定性和恶意行为者会破坏业务的正常运行，因此企业领导者应当为意外事件和不确定性做好准备，并保护驱动业务的价值引擎。而要建立这种能力，首先就需要对能力和漏洞进行严格、客观的评估。组织可以采用“混沌工程”原则来评估风险并理解依赖关系。通过有意损坏系统或移除关键组件，组织可以确定数据、操作、技术和安全能力出现问题的具体位置和方式。

领导者大力加强基本的安全健康措施，为意外事件做好准备。

借助这些信息，并通过跨领域合作来修复缺陷，领导者就可以构建一个富有韧性的技术与运营环境，并更有效地应对中断和保护可信数据。

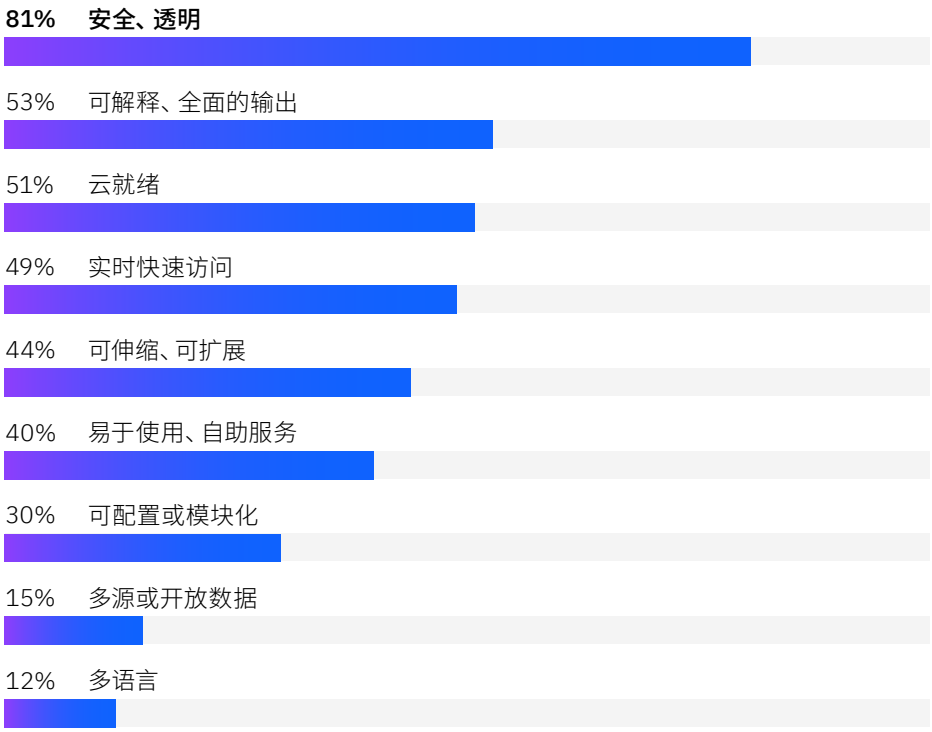
为了实现这一目标，卓越的领导者会优先建立安全、透明的数据架构。根据 IBM 商业价值研究院的调研，超过 80% 的数据价值创造型 CDO 都提到了这一点（见图 4）。[22]

图 4

充分把握商机

安全数据架构让组织能够有效管理风险
并把握新的业务可能性。

数据价值创造型 CDO 最重要的数据架构特征



“安全、透明”远远领先于其他数据架构特征。

信息来源：“全球最高管理层系列 - 化数据为价值：卓越首席数据官事半功倍创造价值”，IBM 商业价值研究院。2023 年 5 月。

观点

回归基础：利用更好的数据清理实践，助力改善绩效

理解数据以识别挑战和商机

组织首先需要评估其运营环境，依据敏感性和重要性对数据进行清点、分类和归类。这包括了解组织如何才能高效地生成符合监管要求的证据。

借助数据分类和管理策略，领导者能够根据数据资产与服务的敏感性和重要性来做出基于风险的决策。当出现不确定性时，领导者可以依靠行动手册来简化决策，并根据可能性或重要性等风险因素来确定补救措施的优先顺序。[23]

保护数据环境以建立和扩展信任

每一家组织都有各自独特的风险偏好。利用风险评估和量化功能来评估风险暴露情况，组织可以向利益相关者传达安全和可信数据的重要性 — 毕竟许多利益相关者都会忽视这一方面。评估现有控制平台（尤其是通过利益相关者的反馈）有助于聚焦于控制可能过于严格或过于宽松的领域。安全遥测和事件日志记录是两项关键能力。

由于许多安全服务开始日益依赖于上下文并由事件驱动，因此组织需要能够熟练地识别用户、设备和日益自动化的服务实体。组织需要将动态风险评分纳入运营，并根据请求是熟悉的还是陌生的、已知的还是未知的、典型的还是异常的，来决定是否提供服务。为此，一些安全解决方案就专门整合了用户与实体行为分析 (UEBA) 或扩展检测与响应 (XDR) 功能。[24]

监控数据环境以提高数据安全性和敏捷性

总的来说，组织需要考虑所有这些因素，以制定更好的数据治理策略和安全控制措施，从而提高数据安全性和敏捷性。标准化和简化数据分类有助于提高效率。降低运营复杂性可以增加数据使用、保护和共享方面的益处。组织可以借服务合作伙伴之力，对其中许多能力进行增强。

为了实现这一目标，许多组织正在使用服务层级来表示数据敏感性和严重性的较高和较低级别，并对可能需要更严格安全控制的供应商进行分类。最后，每一家组织都需要具备经过充分演练的事件响应 (IR) 方案和业务连续性规划 (BCP) 能力。其中必须包括整个组织的利益相关者以及组织外部的关键合作伙伴，例如由营销和传播合作伙伴来传达数据泄露的潜在下游影响。

利用 AI 和自动化

随着 CDO 依靠高级分析和 AI 来发掘数据价值，安全团队还必须利用这些工具来帮助维持和增强组织的安全态势。AI 和自动化技术可以更加有效地自动响应安全事件、识别典型与非典型行为模式以及智能化管理异常与升级。

根据 IBM 价值研究院最近开展的一项调研，AI 安全工具的领先采用者可以更加快速地检测、响应事件并从事件中恢复，其时间只有安全 AI 功能最不成熟的组织的近一半。[25] 全面部署的安全 AI 和自动化是降低与数据泄露相关的总体成本的最重要因素。[26]

但必须要相信 AI 能够充分释放其潜力。新一代 AI（大语言模型，如 OpenAI 的 ChatGPT 工具）具有巨大的潜力，但也引发了有关数据隐私、数据安全和数据伦理的重要问题（请参阅“观点：生成式 AI”）。例如，一些研究人员已经发现了“AI 幻觉”的问题，即模型做出虚假推断或假设不存在的因果关系。

借力合作伙伴

随着组织日益依赖外部业务合作伙伴来增强其能力，安全领导者将这些合作关系视为潜在的威胁向量。不过，通过适当的治理和问责制，外部合作方可以成为加强企业韧性的重要力量。如果合作伙伴秉承共同的核心价值观并坚守责任共担和问责机制，组织就可以将合作网络重塑为对运营意识、风险缓解和冗余能力的共同投资，从而为所有相关方提供安全保障。

明智的合作伙伴战略应当意识到，合作伙伴可以合力加速洞察、降低风险以及捕获新的价值来源。事实上，拥有成熟合作伙伴战略的领先 CDO 组织实现了比其他组织高出 63% 的收入增长率。[27]

在整个组织和合作伙伴网络中建立整合的数据、运营、技术和安全策略有助于建立信任。建立信任之后，组织就可以进一步释放更多价值。

通过适当的治理和问责制，外部合作方可以成为加强企业韧性的重要力量。

观点

生成式 AI 的风险和机遇

风险

根据 Salesforce 最近开展的一项调研，大多数 IT 高管希望生成式 AI 能够帮助其组织更有效地利用数据来服务客户并提高运营效率。但 71% 的受访者预计这会给其组织的数据带来新的安全风险。[28]

尽管 ChatGPT 等工具激发了公众的想象力，但同时也带来了数据隐私问题。例如，一些好奇的用户在向系统提交提示词时可能会向公众公开商业敏感信息。[29]

威胁行为者还可以利用生成式 AI 工具快速生成新的、更复杂类型的恶意软件和网络钓鱼方案。[30] 生成和执行代码的能力应引起每个人的关注，这也正是许多领导者主张谨慎使用生成式 AI 工具的原因。[31] 生成式 AI 工具的输入和输出都可能会受到操纵。当自主 AI 代理被用来生成虚假内容、执行操作或大规模、快速地触发攻击时，这将带来更大的危险。[32]

机遇

生成式 AI 也具有防御优势。生成式 AI 可以模拟攻击，从而增强组织的培训和灾备能力。[33] 组织可以定制大语言模型和基础模型来改进培训和知识管理，例如，通过规划内容来帮助补足技能短板。此外，定制化模型还可以回答审计问题，并生成情报与风险报告，为组织提供更多安全事件背景信息。[34]

在参与生成式 AI 项目时，企业领导者必须确保建立强有力的 AI 伦理和治理机制，从而有效缓解相关风险。为了促进在网络安全中负责任地使用生成式 AI，领导者需要实施可识别攻击和防御用例的安全政策与控制措施。为了充分发挥 AI 的效用，领导者需要开发新的实践方法来监控输入和输出，以防止被操纵。最后，为了建立信任，每一家组织都应当制定关于如何使用和禁止使用生成式 AI 解决方案的指导准则。

另外，企业还可以充分发挥基于 AI 的安全智能的作用。首先，采用与 AI 系统生命周期所需的风险和合规水平相符的全方位监控系统，持续跟踪和评估模型性能、数据使用和合规性。其次，加速在整个企业和合作伙伴网络中采用零信任网络安全框架。这种方法假设潜在威胁可能来自任何来源，从而确保对系统的所有访问均得到验证和监控。最后，利用基于 AI 的安全工具来增强组织检测、预防和响应潜在安全威胁的能力，确保在每个层级（一直到董事会）制定明确的事件升级政策。

国内某银行：数据弹性保护，实现快速检测及恢复

北方某银行具有典型的三站点容灾架构，目前可保障99% 以上物理故障情况下数据不被损坏，但是对于人为错误、逻辑错误、入侵勒索保护不足。

为进一步保证数据安全，IBM 为其增加了数据弹性保护（Safeguarded Copy），增加了 Air Gap 保护。经过系统部署，帮助该银行实现了对于人为错误、逻辑错误、入侵勒索等威胁的保护，3 天内实现数据的快速检测和快速恢复，恢复颗粒度小于 4 小时，配合数据库功能，颗粒度可以更小。超过 3 天的数据可使用磁带库进行恢复。

IBM：携手合作伙伴，构建云上安全运营中心

企业可以借助云上安全运营中心，实现 7×24 小时全天候的安全风险监控和应急响应。

2022年年6月，IBM宣布与全球领先的信息技术服务某公司携手，依托该公司强大的 IT 服务团队和服务经验，以及 IBM QRadar 技术平台，推出基于亚马逊云科技的云上安全运营中心服务，帮助客户快速准确识别安全事件，全面开展调查并及时采取响应行动，有效地保护客户混合多云环境中的重要资产，同时大大缓解客户安全运营人员不足的痛点和挑战。

纵腾集团：数据弹性保护，实现快速检测及恢复

作为全球跨境电商基础设施服务商，福建纵腾网络有限公司（以下简称“纵腾集团”）业务覆盖全球 220+ 国家与地区，在欧美日等发达地区建立 30 多个转运中心，日均包裹处理量超过 140 万件，服务超过 20,000+ 跨境电商客户。随着跨境电商的大爆发，尤其是 DTC（Direct To Consumer）模式的兴起，跨境 B2C 交易额不断走高。除了面临安全合规的挑战，业务迅速扩张带来的大量数据和订单处理，也要求底层基础 IT 架构具备极高灵活性和稳定性来快速响应市场的变化和客户需求。纵腾集团过去采用 IDC 托管式服务，时常会遇到机房空间不足、资源扩展周期长、大量闲置资源浪费的情况。尤其是在跨境电商大型购物促销期间，如“黑五”高峰期，保障系统的稳定性和高可用性是重中之重。

纵腾集团利用 Amazon GuardDuty 持续监控亚马逊云科技环境中的网络活动、数据访问模式和账户行为来识别威胁。除了检测威胁之外，纵腾集团还可以轻松自动化应对威胁的方式，从而缩短补救和恢复时间。在 2022 年“黑五” 大促前夕，纵腾集团通过监控发现系统存储空间被迅速占用，当时总存储空间已所剩无几，为了应对这一突发事件，亚马逊云科技团队迅速提供了 Amazon IEM 响应服务。亚马逊云科技高级支持工程师首先检查了集群节点和关键资源并进行底层排查工作，问题得到迅速定位后，支持工程师立即提供了应对的架构解决方案、推荐资源、展开指导部署。期间，支持工程师还协助纵腾集团的技术团队进行了负载测试，对结果实时审查。在短短 2 小时内，所有问题得到快速解决，全程保障了纵腾集团在业务迎来高峰前系统的稳定性和连续性。

信息来源：亚马逊云科技案例客户案例。2023年,“实力助攻，亚马逊云科技全方位护航纵腾集团抓住跨境电商新机遇”.
https://www.amazonaws.cn/customer-stories/ecommerce/ztn/

行动指南

数据安全成为业务加速器?

组织竞争力背后的无名英雄

企业高管应当采取的行动

对齐战略

与组织的“北极星”保持一致，建立共同基础。

立即行动

– 确保数据、运营、技术和安全策略与组织的核心业务战略（即“北极星”）保持一致。

– 识别合作伙伴和客户的摩擦区域，重点关注阻碍决策、价值实现或信任的制度和治理因素。

后续行动

– 识别高影响力风险并制定跨职能的风险缓解计划，以最大限度减少业务中断。

– 专注于需要协同数据、运营、技术与安全能力做出决策的更高层级的价值主张。

营造文化

营造数据安全可信的企业文化，并将数据安全可信视为实现价值的最快路径。

立即行动

– 激励从董事会到一线员工自上而下的数据安全实践和数据素养。

– 将数据安全重塑为提高绩效的基石（包括更强的信任关系、风险管理能力、决策能力和韧性）。

– 积极与监管机构建立关系，将合规性打造为竞争优势。

后续行动

– 评估安全团队的组成。不要仅关注学位和证书。邀请非安全背景、不同观点、不同种族背景的人士加入对话，建立更完整的安全视角。

– 在每位员工的工作职责中，增加“保护安全和数据隐私”的内容。

– 倡导更强大的数据因素和数据伦理能力所带来的业务价值。

行动指南

职能和业务部门高管应当采取的行动

预测风险

通过增强网络抗风险能力来应对不确定性。

立即行动

– 采用风险量化和评估功能持续评估潜在的受攻击面。

– 转变思维，积极思考“如何实现数据安全目标”，而不是不假思索地对新特性和新功能说“不”。

– 加强数据安全基础和日常安全健康实践，助力安全团队有效应对计划外中断。

后续行动

– 使用混沌工程原则来预测未来的潜在冲击。

– 运用事件响应模拟来锻炼数据、运营、技术和安全团队之间的协同合作能力。

统筹合作

运用集成的数据、运营、技术和安全能力来增强整个合作伙伴网络的网络韧性。

立即行动

– 识别与您的核心价值观和风险管理方法相符的合作伙伴。选择可帮助您实现“北极星”业务目标的合作伙伴，尤其是涵盖数据、运营、技术和安全职能的合作伙伴。

– 部署 AI 和自动化解决方案，以提高数据、运营、技术和安全职能的工作效率。运用 AI 来补充人类的专业知识，并加速网络事件检测、响应和恢复。

后续行动

– 部署合作伙伴级仪表盘，以增加对通用数据、运营、技术和安全实践的可见性和透明度。

– 确保合作伙伴网络的决策与您的“北极星”业务目标相一致，使用公认的治理标准来降低复杂性、简化决策流程以及增强整体的网络安全韧性。

关于专家洞察

专家洞察代表了思想领袖对具有新闻价值的业务和相关技术主题的观点和看法。这些洞察是根据与全球主要的主题专家的对话总结得出。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com

IBM 商业价值研究院

IBM 商业价值研究院 (IBV) 创立二十年来，凭借 IBM 在商业、技术和社会交叉领域的独特地位，我们每年都会针对成千上万高管、消费者和专家展开调研、访谈和互动，将他们的观点综合成可信赖的、振奋人心和切实可行的洞察。

需要 IBV 最新研究成果，请在 ibm.com/ibv 上注册以接收 IBV 的电子邮件通讯。您可以在 Twitter 上关注 @IBMIBV，或通过 https://ibm.co/ibv-linkedin 在 LinkedIn 上联系我们。

访问 IBM 商业价值研究院中国官网，免费下载研究报告：https://www.ibm.com/ibv/cn

选对合作伙伴，驾驭多变的世界

在 IBM，我们积极与客户协作，运用业务洞察和先进的研究方法与技术，帮助他们在瞬息万变的商业环境中保持独特的竞争优势。

致谢

本报告是亚马逊云科技和 IBM 商业价值研究院 (IBM IBV) 的多个团队通力协作的共同成果。我们要特别感谢以下人员为本报告做出重要贡献以及提供指导：Heather Deguzman、Sandra Woods、Teresa Rollins、Dinesh Nagarajan、Bhuvana Chandar、Bob Breitel、Mahmoud Elmashni 和 Liam Cleaver。此外，我们还要感谢编辑主管 Joanna Wilkins 和设计主管 Nancy Pendleton 为本报告贡献的卓越才能和创造力。

关于亚马逊云科技

在过去的 15 年，亚马逊云科技一直是全球最全面、应用最广泛的云平台。如今，我们为数百万计的客户提供服务，从发展最快的初创公司到超大型企业，遍及全球每一个角落的千行百业。我们致力于通过基于云的数字化转型来帮助这些客户发展壮大业务。在此过程中，我们与企业最高管理层密切合作，从独特的视角来了解高管实现数字化转型的不同方式，包括各种最高管理层角色的不同思考过程、他们的态度和优先事项、进展的障碍以及最成功的最佳实践。

关于亚马逊云科技-IBM 安全合作伙伴关系

IBM 是亚马逊云科技一级咨询合作伙伴，依托于 IBM Technology 和 IBM Consulting 提供 3 项安全能力以及总共 16 项亚马逊云科技能力。IBM 与亚马逊云科技携手合作，每天都为超过 100 万客户的首选云平台提供快速、高度安全的开放软件功能。借助亚马逊云科技强大的云原生功能，以及亚马逊云科技 Marketplace 上的超过 50 种 IBM 解决方案，客户可通过交钥匙交付和集成的方式来部署 AI 驱动的 IBM 软件。要了解更多信息，请访问 https://www.ibm.com/aws/security

相关报告

网络经济时代的发展繁荣之道

McCurdy、Chris、Shlomi Kramer、Gerald Parham 和 Jacob Dencik。“网络经济时代的发展繁荣之道：重新思考业务转型的网络风险” IBM 商业价值研究院，2023 年 2 月 https://www.ibm.com/downloads/cas/4MXMDOKA

化数据为价值

“全球最高管理层系列 - 化数据为价值：卓越首席数据官事半功倍创造价值” IBM 商业价值研究院，2023 年 5 月 https://www.ibm.com/downloads/cas/RGNNORK3

2023 首席数据官 (CDO) 议程

Davenport, Thomas H. “Chief Data Officer (CDO) Agenda 2023: Prioritizing business value creation.” AWS. 2022. https://aws.amazon.com/data/cdo-report/

备注和参考资料

1 McCurdy, Chris, Shlomi Kramer, Gerald Parham, and Dr. Jacob Dencik. “Prosper in the cyber economy: Rethinking cyber risk for business transformation.” IBM Institute for Business Value. November 2022. https://ibm.co/security-cyber-economy

2 “Cost of a Data Breach Report 2022.” IBM Security and the Ponemon Institute. July 2022. https://www.ibm.com/reports/data-breach

3 “IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less.” IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo

4 Davenport, Thomas H.“Chief Data Officer (CDO) Agenda 2023:Prioritizing business value creation.”AWS.2022. https://aws.amazon.com/data/cdo-report/

5 “IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less.” IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo and unpublished data

6 Milne, Duncan. “The Brakes Aren’t There to Slow Us Down. What Can Legal and Compliance Programs Learn from the Fastest Sports Teams on the Planet?” The Compliance and Ethics Blog. January 31, 2022. https://www.complianceandethics.org/the-brakes-arent- there-to-slow-us-down/

7 Davenport, Thomas H. “Chief Data Officer (CDO) Agenda 2023: Prioritizing business value creation.” AWS. 2022. https://aws.amazon.com/data/cdo-report/

8 Ibid.

9 Wayner, Peter. “Hot areas for encryption innovation.” CSO. September 28, 2020. https://www.csoonline.com/article/3575830/4-hot-areas-for-encryption-innovation.html

10 “In unpredictable times, a data strategy is key.” MIT Technology Review Insights in collaboration with AWS. https://pages.awscloud.com/GLOBAL-ln-GC-600-SOL-Unpredictable-Times-Data-Is-Key-learn.html?trk=d267b9ce-17c0-4ebc-9f42-24f6e3e4ab26; “IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less.” IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo

11 “IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less.” IBM Institute for Business Value. March 2023. Unpublished data.

12 “Cost of a Data Breach Report 2022.” IBM Security and the Ponemon Institute. July 2022. https://www.ibm.com/reports/data-breach

13 Ibid.

14 《2023 年第一季度我国数据泄露事件仍呈现高发态势》，央视新闻 2023-4-15，https://news.cctv.cn/2023/04/15/ARTI3KybXBjgzq1FAnTltUUb230415.shtml

15 “IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less.” IBM Institute for Business Value. March 2023. Unpublished data.

16 Ibid.

17 Zhadan, Anna. “World Economic Forum finds that 95% of cybersecurity incidents occur due to human error.” January 18, 2022. https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/

18 Subramoni, Santha. “Cybersecurity:Why we need to shift the narrative to build a cyber-ready workforce.” World Economic Forum. February 8, 2023. https://www.weforum.org/agenda/2023/02/cybersecurity-cyber-ready-workforce-training-reskilling/

19 “#125: Think Like an Auditor: How to Measure Security Compliance.” AWS podcast. https://aws.amazon.com/podcasts/125-think-like-an-auditor-how-to-measure-security-compliance/

20 “The Total Economic Impact™ Of IBM Security Guardium: Cost Savings And Business Benefits Enabled by Guardium.” Forrester Research, commissioned by IBM. October 2020. https://www.ibm.com/resources/security/forrester-tei-guardium

21 Paydos, Timothy and Mike Stone. “Preparing governments for future shocks.” IBM Institute for Business Value Blog.July 13, 2022. https://www.ibm.com/thought-leadership/institute-business-value/blog/government-prepare-future-shocks; Scott, Tony, “Preparing governments for future shocks: An action plan to build cyber resilience in a world of uncertainty.” https://ibm.co/governments-future-shocks

22 “IBV C-suite Series. Turning data into value: How top Chief Data Officers deliver outsize results while spending less.” IBM Institute for Business Value. March 2023. https://ibm. co/c-suite-study-cdo

23 “How to Use (And Understand) a 5x5 Risk Matrix.” HASpod. September 20, 2020. https://www.haspod.com/blog/paperwork/5x5-risk-matrix

24 “IBM Security QRadar Suite.” IBM webpage. Accessed May 9, 2023. https://www.ibm.com/qradar; “What is User and Entity Behavior Analytics (UEBA)?” Palo Alto Networks website. Accessed May 9, 2023. https://www.paloaltonetworks.com/cyberpedia/what-is-ueba

25 Muppidi, Sridhar, Lisa Fisher, and Gerald Parham. “AI and automation for cybersecurity: How leaders succeed by uniting technology and talent.” IBM Institute for Business Value. June 2022. https://ibm.co/ai-cybersecurity

26 “Cost of a Data Breach Report 2022.” IBM Security and the Ponemon Institute.July 2022. https://www.ibm.com/reports/data-breach

27 “IBV C-suite Series.Turning data into value: How top Chief Data Officers deliver outsize results while spending less.” IBM Institute for Business Value. March 2023. https://ibm.co/c-suite-study-cdo

28 “IT Leaders Call Generative AI a ‘Game Changer’ but Seek Progress on Ethics and Trust.” Salesforce News & Insights. March 6, 2023. https://www.salesforce.com/news/stories/generative-ai-research/

29 Gal, Uri. “ChatGPT is a data privacy nightmare. If you’ve ever posted online, you ought to be concerned.” The Conversation. February 7, 2023. https://theconversation.com/chatgpt-is-a-data-privacy-nightmare-if-youve-ever-posted-online-you-ought-to-be-concerned-199283

30 Jackson, Terrance. “Exploring The Security Risks Of Generative AI.” Forbes. April 19, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/04/19/exploring-the-security-risks-of-generative-ai/?sh=10d46e993594

31 Metz, Cade. “The Godfather of A.I. Leaves Google and Warns of Danger Ahead.” The New York Times. May 1, 2023. https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton. html

32 Keary, Tim. “How prompt injection can hijack autonomous AI agents like Auto-GPT.” VentureBeat. https://venturebeat.com/security/how-prompt-injection-can-hijack-autonomous-ai- agents-like-auto-gpt/

33 Linthicum, David. “Generative AI and Cybersecurity: Advantages and Challenges.” eWeek. April 10, 2023. https://www.eweek.com/artificial-intelligence/generative-ai-and-cybersecurity/

34 Jackson, Terrance. “Exploring The Opportunities of Generative AI For Improving Security Operations.” Forbes. March 22, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/03/22/exploring-the-opportunities-of-generative-ai-for- improving-security-operations/?sh=769ec03f1d04

国际商业机器（中国）有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编：100020

美国出品 | 2023 年 10 月

扫码关注 IBM 商业价值研究院

官网　微博　微信公众号　微信小程序

WYZMYZAQZHCN-00