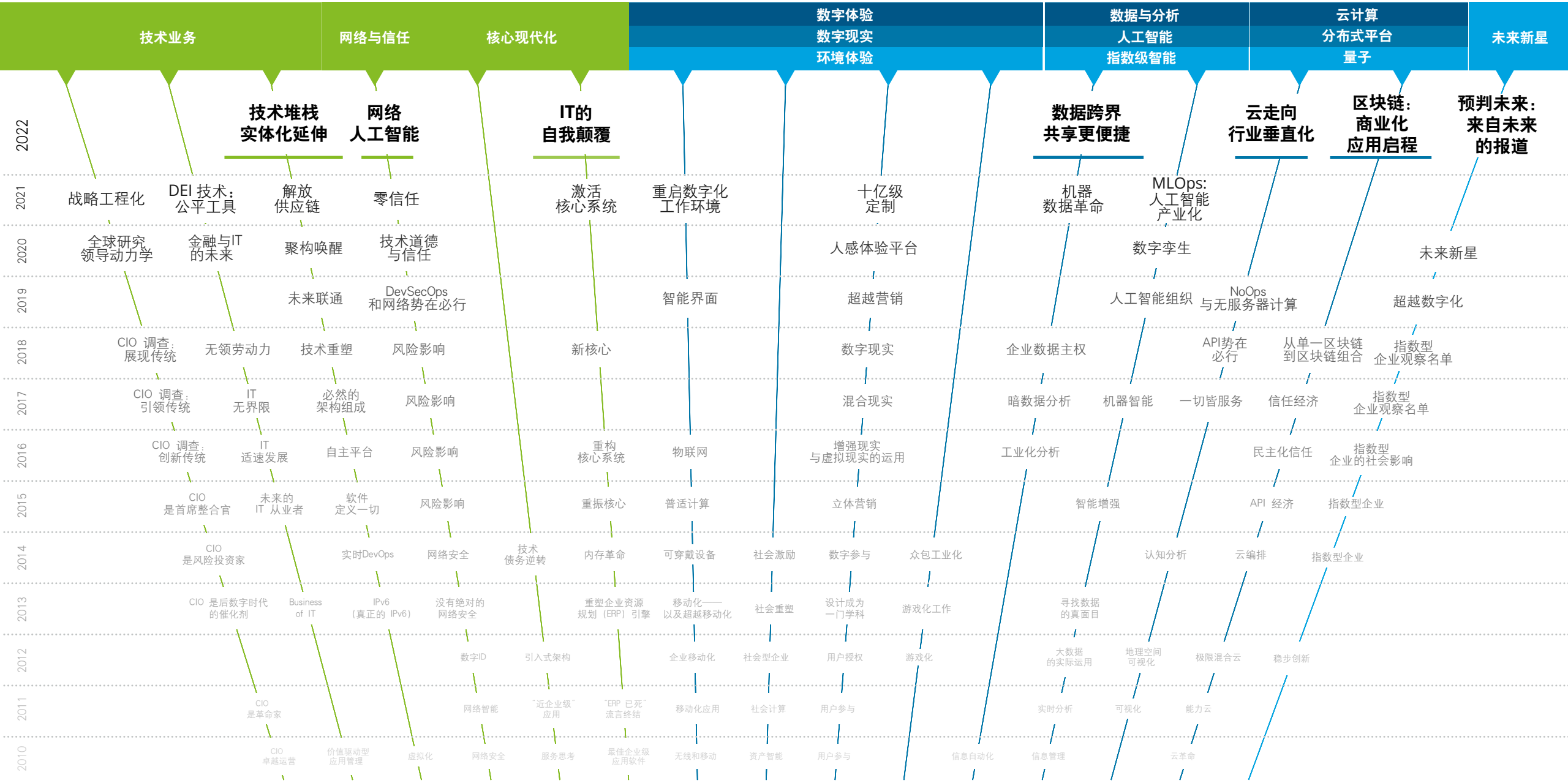
Deloitte.
Insights

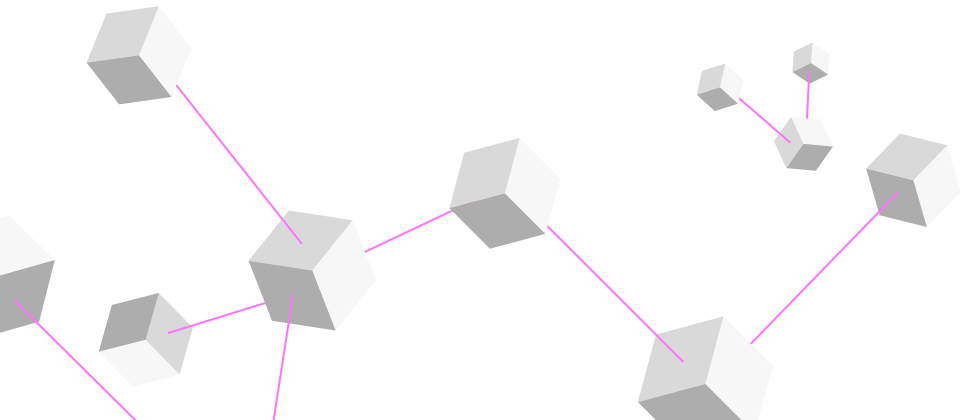
2022技术趋势

中文版

趋势分析：十三年潜心研究



目录



编辑寄语

过去两年新冠肆虐全球，而现在我们众志成城，努力构建“下一个新常态”。作为“技术趋势”团队的成员，我们相信，这是我们创造美好未来的契机——因为我们不仅要延续传统的 IT 发展，还要重新思考如何携手前行。

毫无疑问，前进需要我们每一个人的努力。最好的艺术演绎人们的生活，最优秀的新闻报道表达群众的呼声。无疑，公众一直担忧“机器人帝国”的崛起，这就是为什么我们能看到大量关于这方面的报道。然而事实上，由人工智能辅助的未来，不会是一面暗黑的镜子，也不会是解决一切烦忧的万能药，事情并不是非黑即白。现实是很多组织正在自动化处理繁重的重复性工作，把人类解放出来，专注于解决更有趣、更高价值的问题。如果有什么不同的话，那么就是对于雇主来说员工变得更加宝贵，人才争夺，尤其是科技领域的人才争夺，从未如此激烈。

在今年的技术趋势报告中，我们展示了领先企业正通过不同的方式， 进行自动化、抽象和外包， 将他们的业务流程通过日益强大的技术工具来完成。 我们发现，领军企业利用强大的科技力量，不断武装员工，让他们能够轻松应对创新项目，实现竞争差异化。例如，区块链推动企业实现与第三方之间的流程自动化，从而消除人工数据交换、数据录入和报告的需求，创造“记录即报告”的环境。 IT 部门正将其核心系统基础设施里的大部分内容自动化，让工程师回到实际工程设计中。 人工智能在网络安全领域作用日益凸显——自动检测威胁并做出响应，减轻网络安全人员的负担。

当然，疫情也推动了今年的技术趋势发展，但趋势并非是对新冠肺炎影响的直接反应。与其说疫情重新调整了企业的目标，还不如说它进一步突出了当前优先事项的重要性。企业过去认为我们关注的各项举措会在未来五到十年内实现，但现实是？ 这些问题需要马上解决。 客户希望获得绝佳的数字+实体体验，员工希望可以随时随地开展工作。

那么您的竞争对手呢？过去的对手变得更加高效，新的对手（他们的业务并未与您的业务重合）也在跃跃欲试，想要将您踢出舞台。数字化颠覆者并不是因为规模小才成功的，而是因为他们的架构精简，使其更加果断、敏捷和弹性，所以才能够在竞争中占据上风。为了在当今的环境中蓬勃发展，企业也开始认识到，要想获得更多，他们必须做得越少。这就是为什么他们寻求自动化、分离和外包，并探索支持这些理念的技术要素，如云、安全和数据。

疫情直接挑战了传统意义上的能力极限。它向我们展示了，当生产力障碍消除后，精力得以更集中的员工可以取得多高的成就。在 IT 领域，员工竭尽全力，设置远程工作所需的基础设施，支持全新的客户触达方式，这增强了 IT 的可信度。现在，企业期望技术团队可以推动下一轮创新：找到更大的挑战，并征服挑战。

与此同时，技术团队却觉得自身很不稳定，很少 IT 管理者会认为他们拥有足够的人员。 因此，在充满雄心壮志但资源却有限的世界里，企业一直尝试着以更少的代价获得更多的效益。

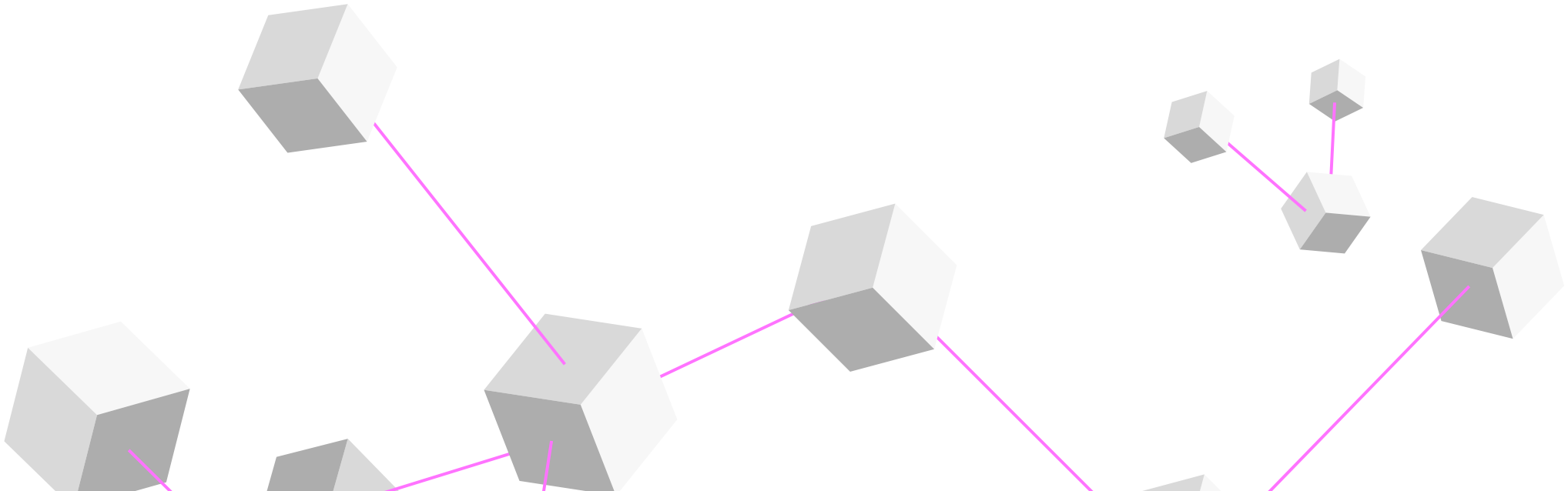
《2022 年技术趋势》将自动化视为可持续发展和增强基础运营的新关键，同时说明了自动化反过来将如何促进员工升级价值链，专注于解决更有价值的问题。

未来属于人类，让我们大展身手吧。

Scott Buchholz
德勤管理咨询
新兴技术研究总监
兼政府与公共服务首席技术官
sbuchholz@deloitte.com
@scott_buchholz

Mike Bechtel
首席未来主义学家
德勤管理咨询
mibechtel@deloitte.com
@mikebechtel

Bill Briggs
德勤管理咨询
全球首席技术官
wbriggs@deloitte.com
@wdbthree



执行摘要

案例分析、洞察和趋势

数据跨界共享更便捷

- CVS Health
- Catena-X
- 美国国防部高级研究计划局 （DARPA）
- Kyle Rourke, Snowflake

云走向行业垂直化

- Marijan Nedic, SAP

区块链：商业化应用启程

- 法国公共金融机构 (Caisse des Dépôts et Consignations)
- 周大福 (Chow Tai Fook)
- 美国财政部 （US Department of Treasury）
- 宝马集团 (BWM Group) Andre Luckow 博士

IT 的自我颠覆：自动化技术的规模化应用

- 美国第一资本金融公司 （Capital One）
- UiPath
- 安森保险公司 (Anthem)
- Bill McDermott and C.J. Desai, ServiceNow

网络人工智能：有效防御

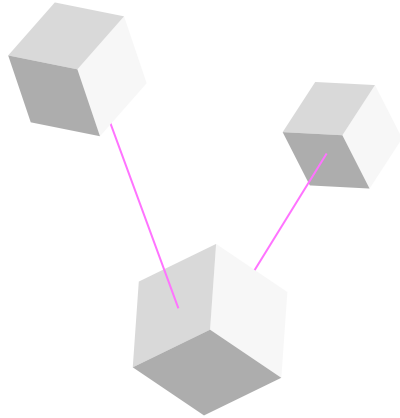
- Sapper Labs Cyber Solutions
- 美国圣母大学 (University of Notre Dame) Mike Chapplee
- 美国陆军 (US Army) Adam Nucci

技术堆栈实体化延伸

- 美国西南航空公司 (Southwest Airlines)
- 南加州爱迪生电力公司 (Southern California Edison)
- 舍巴医疗中心 (Sheba Medical Center)
- Brad Chedister, DEFENSEWERX

预判未来：来自未来的报道

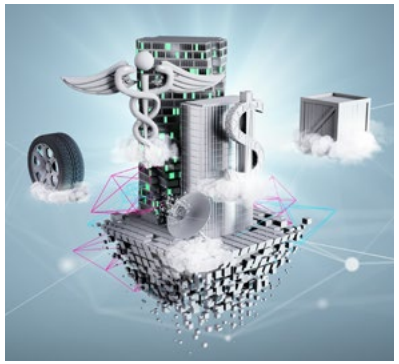
- 德勤 (Deloitte) Mike Bechtel



数据跨界共享更便捷

诸多新技术致力于在保护隐私的同时，简化组织内和组织间的数据共享机制。越来越多的组织开始借助大量以前没有权限获取的外部数据，不断挖掘自身敏感数据的价值，从而实现企业增长。这将带来全新的数据驱动机遇。实际上，在同一个生态系统或价值链内的安全数据共享，将催生新的商业模式和产品。例如，新冠肺炎疫情刚刚爆发时，很多平台共享了临床数据。研究人员、医疗机构和药企通过共享平台汇集临床医疗数据，加快了治疗方法和疫苗的研发。而且，这些数据共享协议还帮助药企、政府机构、医院和药店协同行动，大范围地执行疫苗接种计划，在保护知识产权的同时确保效率和安全。

云走向行业垂直化



数字化转型的重心已经从满足任何行业组织的IT需求，转变为满足具体行业甚至细分行业的特殊战略和运营需求。超大规模云服务商和SaaS (软件即服务) 供应商正与全球系统集成商和客户合作，提供模块化的、行业垂直的商业服务与加速器，这些服务和加速器易于被采用和部署，从而帮助组织打造自身独特的竞争优势。随着这种趋势越来越明显，部署应用程序的过程将从创造 (create) 变成组装 (assembly) ——这种转变可能会令整个价值栈重新排序。业务流程将成为需要购买的战略商品，使组织可以将宝贵的发展资源集中在战略和竞争差异化的关键领域。

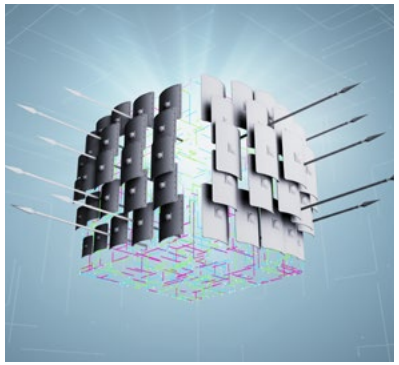
区块链：商业化应用启程

新潮的加密数字货币和不可伪造的代币 (NFTs) 总是占据媒体头条，激发公众想象。不过，这些技术和其他区块链和分布式账本技术 (DLTs) 也在企业中掀起波澜。事实上，区块链和DLT 平台已经走出了技术成熟度曲线的低谷期，正转化为实际生产力。它们从根本上改变了跨组织开展业务的性质，帮助公司重新思考创建和管理身份、数据、品牌、来源、专业认证、版权等有形资产和数字资产的方式。技术的进步和新监管标准的制定，特别是在非公共网络和平台上的技术和标准，促使金融服务机构以外的企业采用区块链和 DLT 技术。随着企业对区块链和 DLT 的适应，各行各业的创造性应用案例纷纷涌现。成熟的行业领袖努力扩大投资组合并创造新的价值流，而初创企业则致力于挖掘振奋人心的新商业模式。

IT 的自我颠覆：自动化技术的规模化应用

技术日益复杂，用户对稳定性和可用性的期望日益高涨，促使部分企业CIO对所在IT 组织进行大刀阔斧的改革。他们怎么做呢？他们借鉴了云服务供应商的经验。他们识别重复的人工流程，并综合运用工程、自动化和自助服务。这样可以缩短时间，加快价值传递，全面提高 IT 技术的有效性和稳定性。这种自我颠覆式的自动化预示了一个巨大的、但仍未被充分认识到的机遇。以前的技术趋势，如 NoOps、零信任和 DevSecOps 拥有一个共同的主题，即将整个组织代码化。从人工管理向工程和自动化迁移，组织可以更有效地管理复杂系统，并通过提高可用性和弹性来改善客户体验。

网络人工智能：有效防御

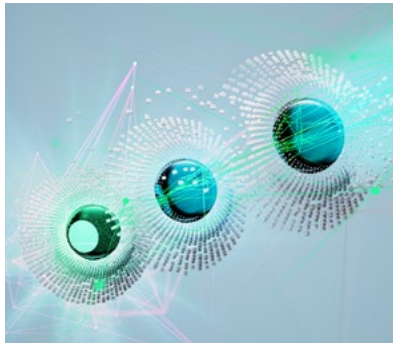


由于检测网络攻击涉及的庞大数据、复杂性和高难度等问题，安全团队可能很快就不堪重负。企业面临的攻击呈指数增长。5G 覆盖越来越广，联网设备也越来越多，更多企业转向远程办公，因此第三方攻击也变得更加致命。人工智能这时候就派上用场了。网络人工智能作为一种加速器，不仅能够帮助组织以比攻击者更快的速度进行响应，还能够提前预判网络攻击，并采取相关防御措施。人工智能可以扩展至新的应用范围，例如用来提升数据分析速度、识别异常、检测威胁。这些新兴的人工智能技术可以帮助分析师专注于预防和补救，并形成更积极、更有弹性的安全态势。而且，如果整个企业都应用了人工智能技术，它也可以用来协助保护宝贵的人工智能资源，阻止人工智能驱动的攻击。

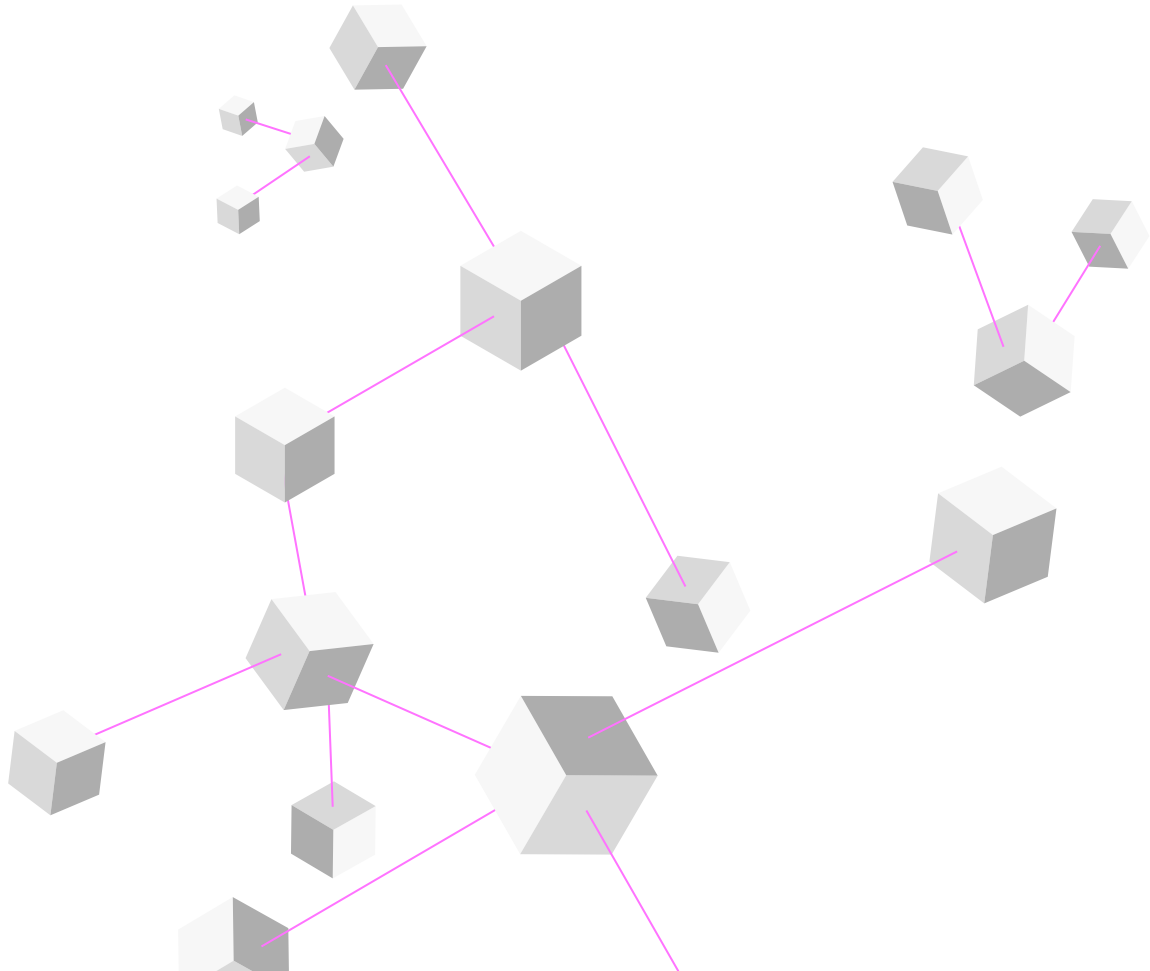
技术堆栈实体化延伸

随着“智能设备”大规模应用以及作业自动化程度的提高，IT 覆盖范围日益扩大，超越了笔记本电脑和手机的范畴。CIO们现在必须考虑如何连接、管理、维护各种各样核心业务资产并保障它们的安全，例如智慧工厂设备、自动烹饪机器人、检查用无人机、健康监测仪等。由于停机可能危及企业或生命，不断演变的实体技术堆栈中的设备对系统正常运行时间和弹性的要求是最高的。同时，可能需要一种新的设备治理和监督方法，来帮助 IT 应对不熟悉的标准、监管机构以及责任和道德问题。最后，CIO可能需要考虑如何招募所需技术人才和重新培养现有员工的问题。

预判未来：来自未来的报道



我们知道，我们将要面临一个充斥各种技术的精彩未来。但是，基于今天的技术发展，我们无法准确预知未来如何发展，以及如何在未来占据优势。我们如何为这种将要发生， 但又不够明朗的事件进行准备和计划？在《2022技术趋势》的最后一章“预判未来：来自未来的报道”中，我们对比了三种技术的发展轨迹。这三种技术分别是：量子、指数级智能 (exponential intelligence) 和环境体验，它们可能会在未来十年或更长的时间内主导整个数字化领域。虽然这些技术目前尚处于起步阶段，但它们都体现了研究人员的创造力，吸引了来自风险投资家、初创企业和拥有以下理念的企业的大量投资：未来一定会发生有趣的事情，通过不懈努力和基础性工作的规划，我们可以做好准备，迎接它们的到来。



数据跨界共享更便捷

共享和繁荣

与他人合并数据，建立数据池，创造新机遇。

数据资产货币化

数据平台提供安全的数据交易机制。

确保数据安全

越来越多的隐私保护技术，有助于保持共享数据安全。

趋势1

数据跨界共享更便捷

强大的数据共享和隐私保护技术开辟了新的数据货币化时代

随着数据共享技术的进步，您可以在高效率的、基于云技术的市场平台上购买和出售具有潜在价值的信息资产。将数据与一系列隐私保护技术结合，如全同态加密 (FHE) 和差分隐私等，您可以共享加密数据并在加密数据的基础上进行计算，而无需对数据进行解密。这样就能达到最佳平衡：在保护安全和隐私的前提下共享数据。

所有这些因素，推动形成一个极具潜力的新趋势。由于隐私或监管问题，存储在世界各地服务器里的，无法被使用的敏感数据，开始以新商业模式和新机会的形式，在企业中产生价值。在未来的 18 到 24 个月里，我们预测，会有更多的组织寻求建立无缝、安全数据共享的能力，拥有这些能力过后，它们可以实现自身信息资产货币化，同时利用他人的数据，达成业务目标。

尽管目前尚处于早期阶段，但数据共享趋势已日益加速。研究机构 Forrester Research 在最近的调查中发现，70% 以上的全球数据和分析决策者都在不断扩大自身利用外部数据的能力，还有 17 % 的决策者计划在未来 12 个月着手扩大数据利用的能力。[1]此外，仅全球 FHE 市场的年增长率就达到 7.5%，预计到 2028年总价值会达到 4.37 亿美元。目前在众多 FHE 应用领域中，最领先的是医疗保健和金融行业。270% 以上的全球数据和分析决策者都在不断扩大自身利用外部数据的能力。是什么推动了这种增长？简单来说，数据在共享时会增加价值。[2]根据 Gartner™ 预测，到 2023 年，积极提升数据共享能力的组织，其大部分业务指标将胜过同行。[3]

70% 以上的全球数据和分析决策者都在不断扩大自身利用外部数据的能力。

目前已有的数据共享示例如下：

- **利用聚合数据安全地实现共同目标。**组织可以与同一市场行业内的“竞争对手兼合作伙伴”团队合作，实现共同目标，如发掘出更深刻的客户洞察，或检测行业内的欺诈模式。
- **提高效率，降低成本。**数据供应商不需要跨企业搭建硬件设施，维护数据库，建立应用程序编程接口 (API)。客户可以一键获取经过匿名化处理后保存的数据。企业内，加密数据使人工智能 (AI) 和机器学习 (ML) 变得更安全，使合规审计变得更容易。
- **扩大研究协作范围。**共享底层基础性或早期研究结果，有助于在不损害辛苦建立的竞争优势的前提下，加快关键性研究项目。
- **保护知识产权。**AI训练数据等超敏感数据可以存储到公共云上，从而得到更好的保护。
- 为动态实时**数据加密。**在高频交易、机器人手术和智慧工厂制造等领域，机密数据需要在多个实体间快速流转。FHE 允许用户无需加密密钥即可获取关键数据。

类似的通过数据共享和聚合来实现数据变现的场景，可以帮助先行的探索者建立竞争优势，这也是目前市场上较受关注的一个方向。 数据共享生态系统的新加入者经常会碰到他们所谓的“哦，天啊”时刻，即发现他们的竞争对手已经在同一平台上进行了很多利用数据资产的尝试。许多会在此刻下定决心成为最出色的 AI 和数据驱动性企业。

共享和相同方式共享

作为数字化转型的命脉，数据在德勤的《技术趋势》报告中占据着极为重要的地位。例如，在《2021年度技术趋势》中，我们讨论了为实现 MLOps 的宏伟目标，公司必须采取不同的方式管理数据。[4] 如今，数据共享革命使组 织能够以更安全的方式，获取其生态系统内的更多数据，甚至跨组织获取数据。但是，要发挥出这样的潜力，同样需要以不同的方式管理数据，此外还要运用创新技术和技能，将信息资产从传统的隐私和安全限制束缚中释放出来。

今年的数据趋势涉及三大维度：**机遇**、**易用性**和**隐私**。

共享和繁荣新商业模式和机遇的前景

共享数据带来共享机遇，创造新的商业模式。随着数据共享趋势的推进，我们预测会有更多的组织参与“数据协作”，以应对共同的挑战，寻求互利互惠的创收、运营和研究机会。此外，这种与外部数据管理服务供应商安全共享数据的能力，有助于组织精简数据管理流程，降低相关成本。参考以下数据共享可能带来的机遇：

- **行业垂直市场**。即便是竞争最激烈的对手，他们也常常需要通过相互协作才能完美应对共同的挑战。以食品行业的供应商为例：如果他们全部都将敏感的销售和交付数据匿名化并加以聚合，用于分析，那么他们就可能更好解决行业的供需难题。 又比如，发展中地区的银行可以匿名化聚合信用数据，建立一套跨银行的信用风险评分体系。再或者一个最大的应用场景，医药研究人员和医生如果能够可以建立一个安全的生态体系数据聚合系统，以更好的理解生命的秘密，更快的将挽救生命的创新应用更快的推向市场？

随着数据共享趋势的推进，我们预测会有更多的组织参与“数据协作”，以应对共同的挑战。

- **同一价值链中的合作伙伴**。许多制造商和零售商从第三方数据公司购买消费者数据，但数据的质量往往不够好，不足以发挥作用。假如同一价值链内合作性质的系统（从供应商到制造商，再到市场营销商）能够合并池化消费者数据，形成更细致的需求图，那么将会怎样？
- **外包 AI 模型训练**。AI 模型往往被认为是高度敏感的知识产权形式。由于它们可安装在一个U盘上，这就表示安全风险较高，所以许多组织一般选择内部自行建模。得益于加密技术，这种模式可能会发生改变。利用安全的建模数据，首席数据官可以将 AI 建模和训练安全地外包给第三方。
- **数据供应商简化交付**。在数据共享平台上，实时市场或物流数据使用权的购买非常简单，一键即可完成。数据供应商无需提供 API 或发送文件。

一键轻松获取外部数据

基于云的数据共享平台帮助组织无缝共享、购买和出售数据。这些高度虚拟化的高性能数据市场通常采用“数据共享即服务”的模式，在这种模式结构中，服务订阅者（也即用户）可以管理、保存和定制数据。他们还可以利用平台自带的“数据净室”（Clean room），保证自身数据达到一定的安全程度。“数据净室”是一种安全空间，附有明确的使用指南，组织可以在这个空间内聚合其数据资产，进行分析。最后，用户可以聚合数据并将其数据使用权出售给平台上的其他用户。数据购买者可以获取市场、产品或研究等不同方面的常规或定制化观点。

这种“共享即服务”模式的底层逻辑是基本的商业战略。这种战略在音乐文件共享和社交媒体等较受人瞩目的信息和内容共享领域的成功，已经证明了其效用。在这种模式下，供应商负责搭建易于使用的数据共享平台，客户提供内容（数据）。[5]

数据市场行业目前正处于“淘金热”的初期阶段，Databrick、Datarade、Dawex 和 Snowflake 等初创公司以及 AWS、Azure、Google 和 Salesforce 等超大规模云服务商正在激烈厮杀，试图在这一极具潜力的市场中占据主导地位。最具前景的是：伴随着数字化转型，数据增长和数据民主化的相互促进，正在推动一场数据革命，使得对外部数据的需求快速增长。[6]数据不再仅仅是影响管理者决策的工具，现在已经发展成为一种可以出售、采购、交易和共享的关键业务资产。那些能够以最便捷、最有效的方式促进此类交换的平台，将最终成为行业数据垂直领域，乃至整个市场内数据共享的标准。

随着越来越多的组织开始寻求机会去实现数据资产货币化，并不断扩大发展其数据资产时，我们看到数据共享的应用场景快速增加，其中一些已经获得成功。例如：

- 在新冠肺炎疫情初期，竞争激烈的全球制药公司探索各种办法，通过数据共享平台，共享临床前研究数据。[7]
- 新冠肺炎疫苗接种单位利用国家管理的集中平台，与公共卫生保健机构共享每日接种和测试数据。[8]
- 一家全球金融服务公司的投资经理实时获取和分析来自后台、中台和前台的数据，从而，与客户共享投资数据所需的时间从“几个月”缩短到了“几分钟”[9]

对于数据共享平台市场的某些方面究竟会如何演变，还需要时间来佐证。但最终必定需要一些整合和标准化处理，不过到时若干平台市场可能已经站稳脚跟。例如，私人数据市场可能会出现合作性质的系统，或者公共市场会涌现迎合特殊需求的产品。无论最终数据市场的形式如何，我们预测，该领域的淘金热将继续如火如荼地展开，尤其是随着供应商开发出钢铁般牢固的安全方案，以及越来越多的组织加入平台，可供消费的外部数据会越来越多。

在不损害隐私的前提下共享数据

数据在共享时增值。但过去的数据隐私政策和竞争性保密需求阻碍了人们实现这一价值的能力。如今，一系列新的计算方法（统称为隐私保护计算，或机密计算） 应运而生，解开了组织及其数据的“隐私”枷锁。利用 FHE、差分隐私和函数加密等方法，组织可以在不损害隐私的前提下，通过数据共享获益（图 1）。

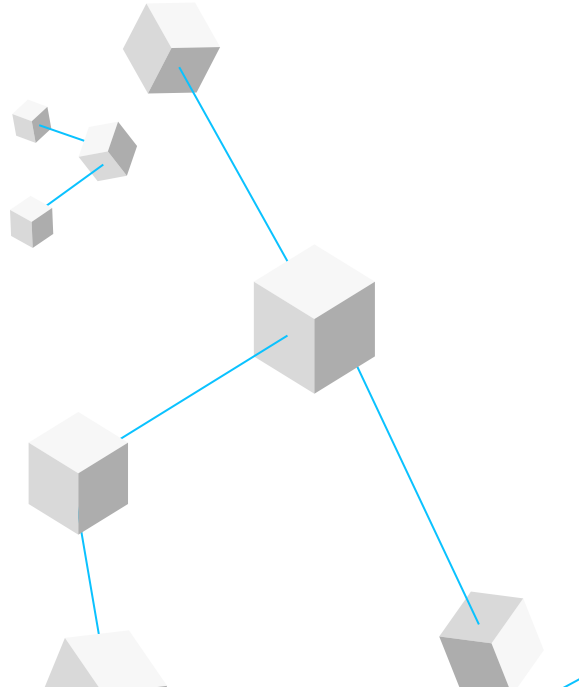
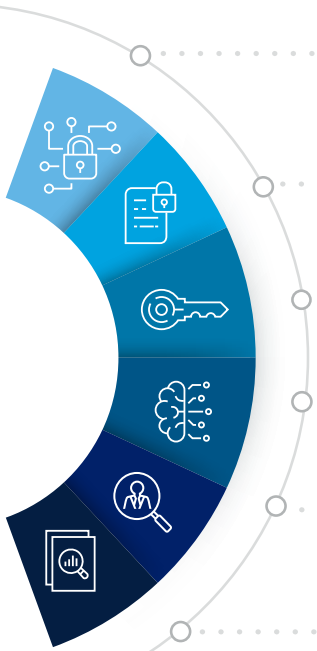


图 1

共享数据的六种隐私保护技术



全同态加密：数据在共享前加密。数据可以分析，但无法解码回原始信息。

差分隐私：在数据集中添加噪声，使其无法还原为原始输入。

函数加密：选定拥有密钥的用户，允许其查看某些部分的加密文本。

联合分析：各方共享其分析见解，而非数据本身。

零知识证明：用户可以在不透露某价值本身的情况下，证明其知晓该价值。

安全多方计算：数据分析会在多方之间进行，因此任何一方都无法单独看到完整的信息。

资料来源：德勤管理咨询研究和分析报告。

隐私保护技术也能促进竞争对手之间的合作。比如不同金融服务领域中相互竞争的多家金融机构，尽管它们会争夺客户，但为了实现检测过度集中风险、复杂欺诈手段或金融犯罪等共同目标，它们也会想要谋求合作。

另一个例子是那些不存在竞争但属于一个行业（如旅游）内互补公司的组织会出现一些具有共同业务价值的数据共享场景， 比如航空公司、酒店和租车公司共同提供信息以推动联合市场营销和促销市场活动。所有参与的公司都想要了解其他公司的客户行为和活动，以便为自己的最终客户带去更多价值，优化客户体验。不过每家公司都有责任保护好客户信息。隐私保护计算可能会是起到突破性作用的催化剂，帮助这些公司展开更深层次的互动和合作。目前，隐私保护计算领域的进展面临着四大挑战

1. 许多相关技术要求有新的软件工具和变革才能利用数据，而要充分利用这些工具并支持这些变革则可能需要工作本就应接不暇的团队投入大量时间和精力。

2. 某些情况下，隐私保护技术会影响速度和性能，这可能会在动态数据及实时分析与传播过程中变成棘手的问题。

3. 对于已经移交到别人手里的数据， 目前没有简单的方法保持对数据治理和使用的控制，这就会增加潜在的隐私或合规风险。

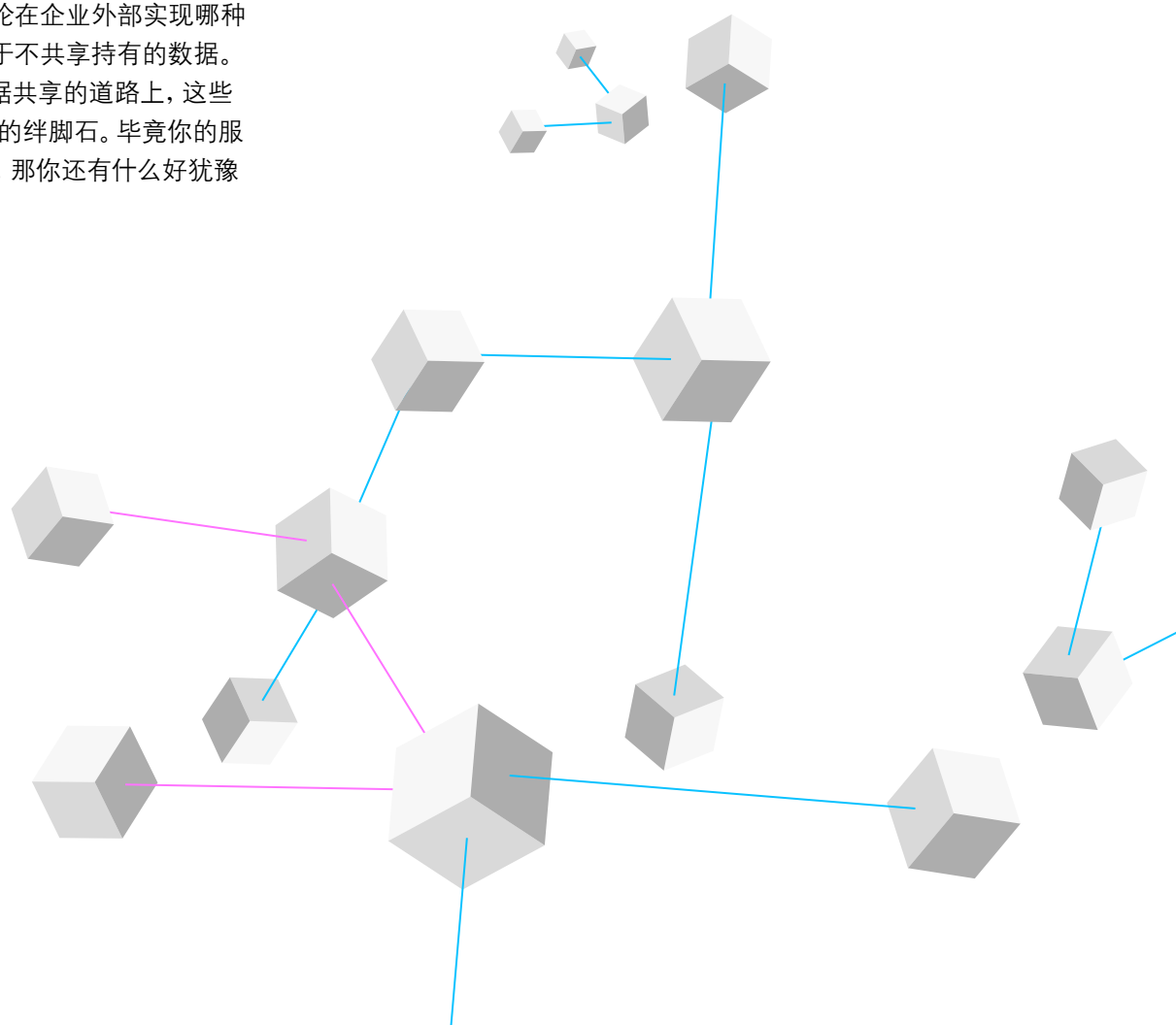
4. 最后，在隐私和数据所有权方面存在着一定的监管障碍，这将影响隐私保护计算充分发挥其商业潜力。

不过，针对所有这些问题的工作都已开始，而且可以比较合理地预测，隐私保护计算在未来 18 至 24 个月将催生大量实践和机遇。

未来的方向

尽管隐私共享计算和先进的数据共享技术使得走在这一趋势前沿的组织不断从数据中提取更多价值，但它们并不能满足所有数据管理要求，也不足以应对所有挑战。你仍然需要强大的数据治理能力，标记和元数据依然必不可少。

另外，新工具和新方法不会一夜之间改变公司长久以来的数据文化。例如，成熟的公司针对数据管理和数据使用通常有着根深蒂固的流程和标准，而初创企业和数字化原生企业则可能会采取更具弹性的方法。家族企业则由于特殊的人际关系影响着决策和战略，无论在企业外部实现哪种程度的数据匿名，此类企业都倾向于不共享持有的数据。我们认为，在通往新时代变革性数据共享的道路上，这些问题以及类似的问题只不过是小小的绊脚石。毕竟你的服务器中就有着一个尚未开发的资产，那你还有什么好犹豫的？



先行者经验

CVS基于数据供应疫苗

CVS Health在美国各地拥有近 1万家门店，每年都成功完成流感疫苗和其他疫苗的接种工作，在这个基础上， 该公司在新冠肺炎疫苗供应方面做出了重大贡献。2021 年春季，当新冠疫苗开始大面积上市时，这家医药零售巨头需立即做出分析，以了解最需要疫苗的地区和时间。 CVS零售数据工程高级总监 Karthik Kirubakaran 表示，该公司数据管理流程和技术成功应对了这一挑战："因为我们拥有有效的数据策略，所以我们能够在几周而不是几个月的时间内扩展我们的能力并推出新的系统。"[10]

Kirubakaran 及其团队收集了来自疫苗供应商以及美国疾病控制与预防中心 （CDC） 的外部数据来预测供需情况。之后，他们将这些信息输入内部系统，以支持患者进行预约、合作伙伴搭建诊所，分析师衡量防疫活动有效性。该团队还与外部研究机构和高校共享数据，帮助评估疫苗接种率。他们在疫情期间以前所未有的速度完成了所有这些工作。幸运的是，CVS的数据组织能力使其能够快速理解输入的数据，与此同时，数据共享工具也保障了安全和近实时的数据交换。Kirubakaran说："我们通过创建横跨多个平台的数据网络快速取得进展，而不是局限于某一项单一技术。"

该团队迅速建立起管理系统，并将数据保护以及隐私和数据安全合规性放在首位。他们还明确了所有者和管理人，并为传输和存储的数据创建了不同层级的安全措施。例如，该团队利用第三方 "净室" 技术将数据匿名，从而支持分析人员根据人口分布区隔而非个人身份衡量疫苗供应计划的成效。

随着疫苗的持续供应，CVS 也面临着新的挑战。每次继续向零售店铺供应疫苗之前，Kirubakaran 的团队成员都会聚在线上策划室内分析人口分布和需求数据，以判断哪些地区供应不足。Kirubakaran 说："我们的预测必须尽可能准确，让需要疫苗的地方能够得到供应。" 后来，他的团队根据每家店铺的供应信息改进了预测方式。为了解有哪些地区疫苗需求量大，他们甚至还分析了互联网上关于新冠肺炎疫苗的搜索。

随着疫苗接种速度减慢，CVS 计划将共享数据用于其他领域。例如，Kirubakaran 的团队正在尝试使用实时数据了解客户在零售店购买的商品，并与客户过去的购买行为进行匹配，从而在结账时更精确地提供优惠券。他所遵循的一条在 CVS 发挥着指导性作用的理念就是，所有 CVS 员工都应该将客户视为他们的服务对象而不是销售对象。Kirubakaran 说："这一理念旨在为社区服务，为客户带来流畅的体验，而且只获取客户允许我们访问的数据。"

Catena-X 变革汽车价值链协作模式

欧洲汽车制造商所在的行业十分成熟，它们的生产制造是基于精密计划和长期优化后的JIT生产方式， 这种模式很难应对过去一年中疫情带来的各种不确定性。 面对新冠肺炎疫情带来的供应延迟和芯片短缺的双重危机，欧洲汽车行业需要迅速做出反应，但从供应商到客户再到回收商，整个汽车价值链的信息都十分割裂。包括宝马和西门子在内的几个主要制造商、供应商和科技公

司因此联合起来，设计了一种新的工作方式。28 个合作伙伴共同推出了 “Catena-X” ，这是一个数据交换生态系统，使各个组织能够按照自己的条件共享信息，同时保护隐私和保障安全。Catena-X 联盟的负责人Oliver Ganser说：“我们需要一个能与价值链上的伙伴展开合作的平台，一个开拓全新竞争领域的平台。”[11]

Catena-X 是 “链” 的拉丁语，该系统于2021年8月推出，是欧盟联合安全数据共享标准 (GAIA-X.[12]) 的首批主要使用案例之一。这种去中心化的方法涵盖多个遵循统一欧盟标准的独立平台。使用 GAIA-X 的组织可以在维持数据主权的同时进行数据交换和跨部门协作。Ganser说：“我们可以放心地把数据放到 GAIA-X 框架中，而无需公司自行建立信任关系。” GAIA-X提供了所需的标准，小型和大型企业最终决定加入 Catena-X 以解决它们应对的供应链问题。在某个案例中，一家汽车制造商发现了一个可能影响到其数万辆汽车的质量问题。这种情况下通常会大规模召回问题车辆，而且供应商可能会遭受数百万的罚款。但通过与供应商合作共享数据，制造商能够准确识别质量问题，并减少超过 80% 需召回的车辆数量。[13]

在不久的将来，Catena-X 将提供用户友好的系统环境，与企业资源规划集成以传输数据，并且还会提供软件即服务型门户网站供小型供应商直接上传数据。随着新企业的加入以及价值链上多元合作伙伴的联手，Catena-X 联盟预计将能创造新的商业模式。例如，合作伙伴可能会针对带有特定参数的共享数据支付奖励费用，另外，可持续性和循环经济也是主要的应用领域。Ganser说：“各组织加入最主要的原因就是想要通过共享数据来解决复杂的业务问题，数据货币化并不是我们首要考虑的问题。”

Catena-X董事会意识到，对于像德国制造业等历史悠久的行业而言，变革可能会很困难。 Catena-X 董事会成员兼西门子公司总监 Claus Cremers 说：“这不仅仅是技术，这是汽车行业的变革。”[14]董事会致力于重新思考价值链作用，鼓励成员转向创业思维。董事会的最终目标是要将这种合作方式从欧洲延伸至全球。Ganser说：“我们会继续生产汽车，但我们可以重新打造整体业务运营的模式，而不是依靠过去的方法。”

DARPA 推动数据加密技术发展

美国国防部高级研究计划局 (DARPA) 一贯致力于推动新兴技术发展。该机构隶属于美国国防部，它赞助的研究项目帮助创造了从互联网、个人电脑到无人机、GPS 等各项技术。目前，DARPA 正在研究共享数据的同时降低隐私和安全风险的新方法，以支持云计算和其他虚拟网络的发展。DARPA 项目经理 Tom Rondeau 博士认为，通过隐私保护技术建立信任是实现民主观念的关键。Rondeau 说：“在保护隐私和保障安全的前提下共享信息是民主的基础。”[15]

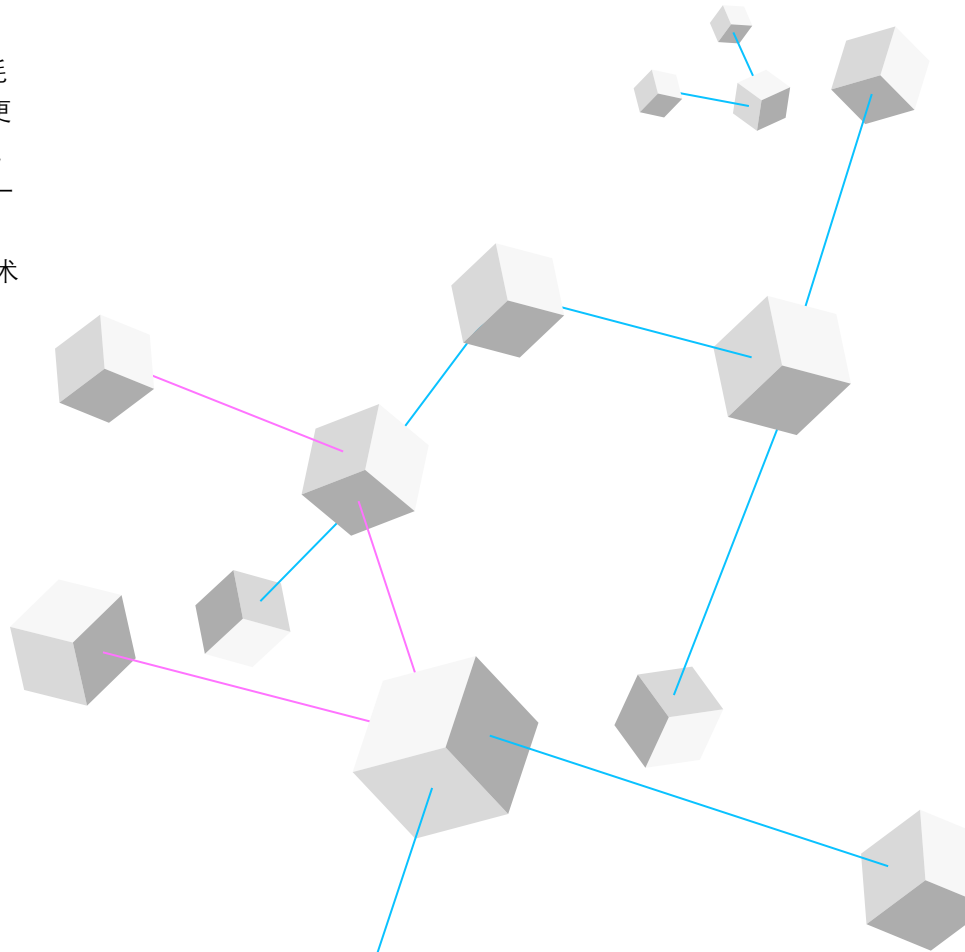
Rondeau领导了虚拟环境数据保护 (DPRIVE) 项目，该项目资助初创企业和现有企业创建能够实现先进加密技术的硬件。标准加密技术可在数据运输或存储过程中确保数据安全，但用户必须解密数据才能用作计算用途，这就会受到网络威胁的影响。相比之下，DPRIVE 重点采用全同态加密 (FHE)，该技术即使在计算过程中也能保护数据。目前，将

FHE 技术应用于敏感数据存储可能需要耗费数月的计算时间。DARPA 的目标是通过开发专用芯片和协处理器来大幅度缩短这一时间。这一隐私保护技术一旦实现并嵌入到手机和平板电脑中，就可以通过每台消费者手中的设备， 安全地收集和存储数据，而且只会加密数据才会发送到其他地方进行分析。Rondeau说："如果我们能够加快 FHE 的运行速度，这项技术可以成为我们几乎每个应用程序数据处理方法的基本组成部分。" 通过FHE，DPRIVE团队正在按严格程度（即计算难度）创建安全标准，因此用户知道他们的数据有多安全。

根据Rondeau的说法，对安全等级的理解应该像购买保险柜一样。保险柜的安全级别依据熟练的窃贼需要花费多长时间破解密码来划分。保险柜的安全等级方便买家根据物品贵重程度来选择合适的保险柜。同样，如果数据管理团队知道黑客破解不同类型的加密信息需要多长时间，他们就可以确定哪些信息需要最高级别的安全防护，以及更改密码的频率，从而防止黑客入侵。Rondeau 说："我们需要能够明确证明某样东西有多安全，这不只是为了让消费者在使用设备时感到放心，也是为了更好地衡量国家安全。"

DPRIVE提供了与其他政府共享国家安全威胁数据的重要用例。Rondeau说："FHE可以成为共享现场情报数据的方式，同时保护获取情报的来源和技术。" 同样，在进行金融犯罪分析时，执法机构需要数据分析犯罪活动，与此同时，银行也有权保护客户的数据。Rondeau认为，先进的加密技术可以帮助双方在不侵犯隐私的前提下共享和分析用于识别洗钱活动的数据。

目前的 FHE 计算是非常密集的计算，对于许多用例而言耗时太长。尽管 DARPA 正与合作伙伴进行合作，试图通过更好的硬件解决这一技术问题，使扩大该解决方案的应用规模则是 DARPA的最终目标。Rondeau 和他的团队认为，一旦隐私保护技术、方法和标准成为常态，随着时间的推移，它们将有助于保护每个人的隐私。Rondeau 说："这一技术能够体现和传达我们在信息安全和隐私方面的民主原则。它能为我们带来诸多好处。"



我的观点

Kyle Rourke

Snowflake公司全球平台战略副总裁

随着绝大多数企业计算向超大规模云服务商转移，全世界的数据正通过云服务商整合到少数物理数据中心内。

然而，单靠这种转变并不能使访问和解锁数据变得更容易，以实现跨组织的数据货币化。Snowflake 在十年前便认识到，要想高效共享和利用数据，组织需要成为相互信任和共同治理网络的一部分，并由能够打破数据孤岛的技术作支撑。

Snowflake 一直都致力于赋能组织在云端存储和分析数据。随着客户不断实现更卓越的性能和并发收益，他们也将目光投向更多数据，甚至包括其他组织拥有的数据。我们在去年推出了我们的基础技术，它创建了一个单一的网络，类似于一个巨大的关系型数据库，或者说数据社交网络，每个客户都可以与该网络连接。各组织只需在平台内授权，就能够根据自己的意愿与其他组织实时共享数据。我们也亲眼目睹了进行合作的组织数量迅速攀升。

通过与其他组织共享或整合数据，许多组织目前正在开发各种创新产品和服务。例如，收集位置分析数据的公司只需点击一个按钮便能将数据发送给共享出行公司，以便于后者知道哪个地方对司机需求最大。媒体出版商可以通过整合自己的消费者数据和零售商的数据，形成一个新的数据集，使双方都能更准确地找到投放广告和销售产品的对象。未来，数据网络可以像社交网络一样发展：用户指数级增长的数据网络将以前所未见和意想不到的方式推动价值创造。

整个行业的数据共享方案正在发生变化。过去，为确保数据收集符合政策规定等，组织必须找到收集数据，复制数据以及将数据上传到服务器的安全途径。随着实时数据（Live data）市场不断发展，组织可以购买或销售数据作为服务，同时免去分析、维护以及合规所需的成本。由于这种方式遇到的阻力越来越小，组织因此可以拥有更多创造性。以前只储存在一家公司内部的数据现在可以供许多公司使用，而未来还会出现其他新颖和有利可图的应用方式。

当然，组织在没有隐私措施的情况下不能共享大多数数据。与我们的数据网络类似的技术需要具备强有力的治理能力以促进信任和推动共享意愿的产生。“净室”将来自多家公司的数据汇集到一起，根据数据安全保障指南进行联合分析。对查询操作进行限制可以防止对个人身份信息等敏感数据的挖掘，同时分析人员也能将收集的匿名记录输入到模型中。

最终，使用企业外部的数据进行分析或创建模型将成为普遍能力。我们的客户在探索不同数据协作途径的同时也在不断为我们指引着前进的方向。目前我们所看到的变化类似互联网如何解锁和民主化地获取信息：以安全、合规、互信的方式围绕数据进行协作和运营的能力将为企业开辟全新的可能性。

高管视角

战略

首席执行官需要密切关注在数据共享下出现的新兴商业模式如果今天的数据交换平台成为下一代条码技术，可能会出现数据货币化或开放新合作伙伴关系的机遇。决定是成为新数据模式的早期进入者还是快速追随者将十分重要。根据对其业务的意义，在早期参与这一趋势可以有力的影响如何完成数据共享的条款。

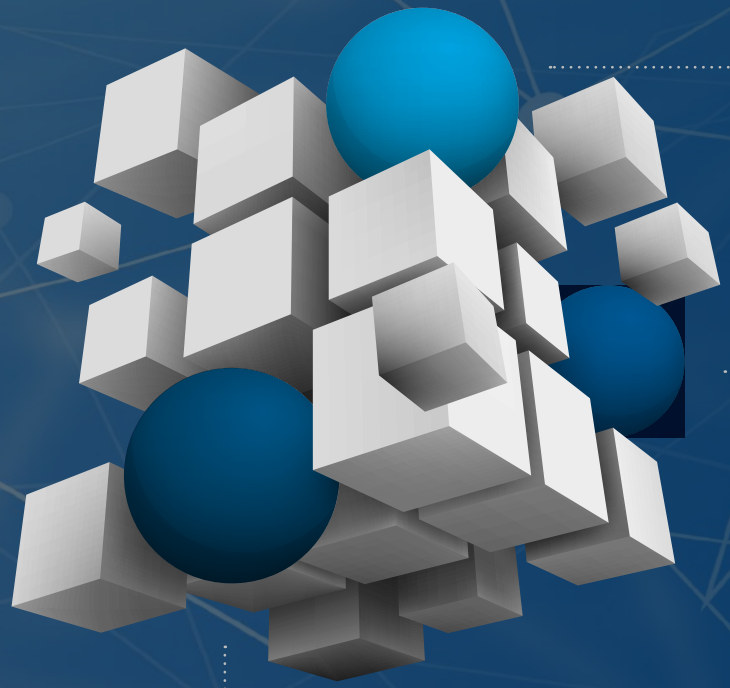
财务

一些首席财务官看到数据共享的趋势可能会感到不安，担心公司的市场竞争力、监管合规性和声誉会受到威胁。然而，随着新的数据共享业务模式的增长，为识别合适的共享机遇,首席财务官将不得不与其他面临相同技术和风险挑战的竞争对手展开合作。随着这一趋势的扩大，首席财务官应权衡数据共享的长期利益和风险，因为这可能事关组织的发展甚至生存。

风险

在过去的一年里，备受关注的网络攻击已经导致整个供应链停摆。随着供应网络和攻击范围的扩大，第三方风险管理将比以往任何时候都更为关键。首席风险官需要与 IT 团队合作，在供应商网络中强调共享数据、安全漏洞和标准规范的重要性。通过推动更高的风险意识，首席风险官可以帮助组织未雨绸缪，并使用最新的隐私保护和安全技术应对未来供应链风险。

你准备好了吗?



关键问题

1 为应对共同挑战，寻求共赢的收益、运营和研究机会，你可以与合作伙伴共享哪些数据资产？

2 你是否利用过数据市场平台的外部数据来增加自己的数据资产？获取更多信息从哪些方面对你的决策过程起到促进作用？

3 你正在使用哪些隐私保护计算技术？分析匿名数据的能力如何（或者是将如何）开辟新的用途和实现创新型实验？

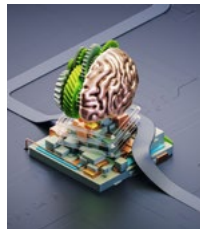
了解更多

数据即战略资产

了解将数据作为战略资产的组织如何在效率、洞察和能力方面实现突破。

机器数据革命

探讨为内部机器消费调整数据如何有助于实现人工智能和 MLOps 效益与规模。



MLOps: 人工智能产业化

深入了解如何应用工程学科来实现机器学习模型开发、维护和交付的自动化。

作者

我们的洞察可以帮助你把握新兴趋势的机遇。如果你在寻找应对挑战的灵感，那我们可以谈一谈。

Frank Farrall

德勤管理咨询
人工智能生态系统负责人
frfarrall@deloitte.com

Nitin Mittal

美国人工智能战略发展
产品负责人
德勤管理咨询
nmittal@deloitte.com

Chandra Narra

德勤管理咨询总裁
cnarra@deloitte.com

Juan Tello

德勤管理咨询首席数据官
jtello@deloitte.com

Eli Dow

德勤管理咨询
分析与认知技术院士
elimdow@deloitte.com

资深撰稿人

Tiago Durão
合伙人
Deloitte & Associados, SROC S.A.

Marcin Knieć
总监
德勤波兰

Rajeev Pai
总监
Deloitte MCS Limited

Markus Schmidthuysen
总监
德勤管理咨询

Vivek Shrivastava
合伙人
德勤印度

Rajeev Singhal
合伙人
Deloitte & Touche LLP

Yves Toninato
高级总监
德勤比利时CVBA

Jeroen Vergauwe
合伙人
德勤比利时CVBA

Dinesh Dhoot
专家领导人
德勤管理咨询

Lakshmi Subramanian
高级经理
德勤管理咨询

Karl-Eduard Berger
经理
德勤法国

尾注

1. Jennifer Belissent, *Chief Data Officers: Invest in your data sharing programs now*, Forrester, March 11, 2021.
2. Data Bridge Market Research, *Global fully homomorphic encryption market – Industry trends and forecast to 2028*, March 2021.
3. Laurence Goasduff,"Data sharing is a business necessity to accelerate digital business," Gartner, May 20, 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
4. Christina Brodzik, Kristi Lamar, and Anjali Shaikh, *Tech Trends 2021: Disrupting AI data management*, Deloitte Insights, December 2021.
5. Michael Gorman,"Data marketplaces will open new horizons for your company," *VentureBeat*, December 23, 2020.
6. Tomas Montvilas,"Understanding the external data revolution," *Forbes*, June 25, 2021.
7. Dr. Nicola Davies,"Covid-19: The importance of data sharing within the pharma industry," Data Saves Lives, June 26, 2020.
8. California Immunization Registry,"Covid-19 vaccine reporting information and resources," California Department of Public Health, accessed November 5, 2021.
9. Snowflake,"State street accelerates investment insights by building alpha data platform," accessed November 5, 2021.
10. Karthik Kirubakaran (senior director of retail data engineering at CVS Health), phone interview, September 22, 2021.
11. Oliver Ganser (head of the consortium, Catena-X) and Claus Cremers (board member of Catena-X) interview, September 15, 2021.
12. Gaia-X,"What is Gaia-X?" accessed November 18, 2021.
13. Ganser and Cremers interview.
14. Ibid.
15. Dr. Tom Rondeau (program manager at DARPA), phone interview, October 26, 2021.

云走向行业垂直化

攀登堆栈

云服务供应商对不断增长的订单业务流程进行自动化和抽象化，以创建行业优化平台。

加倍重视差异化发展

通过云采购商品行业流程，首席信息官可以将人才资源和预算的投入重点放在打造竞争优势的系统上。

建立变革能力

云能力帮助组织通过少量行动打开视野。更少的定制化代码也就意味着更多灵活性。

趋势 2

云走向行业垂直化

行业云解决方案帮助组织将手动任务自动化，将重心转移到具有竞争力的差异化方面

行业云解决方案帮助组织将手动任务自动化，将重心转移到具有竞争力的差异化方面随着全球经济背景从疫情大流行向着未来地方性疫情转移，许多组织都在寻找机会，试图将业务流程转移到云端来提高灵活性和效率。[1]

作为回应，云服务巨头、软件供应商和系统集成商正在开发一系列基于云的解决方案、加速器和 API，这些都是预先配置好的，以支持行业垂直领域的常见场景[2]。这些解决方案是专门为易于采用而设计的，并且可以在其基础上进行构建以实现数字差异化。无论这些产品中的自选应用、工具或服务用户怎样组合，云技术都能将它们连接到一起，形成强大的业务流程解决方案。

例如，一家全球汽车制造商与云供应商合作，为运输业开发基于云的联网汽车应用开发服务。该平台具有行业针对性解决方案，以及物联网、机器学习、分析与计算服务，制造商可以利用这些服务为车辆开发连接层。[3]医疗保健行业最开始部署了云流程来管理后台数据。

随着医疗保健机构开始在云端管理患者数据，1996 年《健康保险携带和责任法案 (HIPAA)》的监管合规性推动该行业云技术应用进入下一阶段。今天，医疗服务供应商先驱正在探索如何使用基于云的 HIPAA 模式改善医疗服务。[4]

在未来 18 到 24 个月内，我们预计越来越多的市场组织将开始探索使用行业云满足其独特的垂直需求的办法。实际上，根据德勤管理咨询的分析，我们预计未来五年行业云市场的价值将达到 6400 亿美元。[5]

显然，云走向行业垂直化的趋势正在增长，而现在正是为你的组织探索可能性的时候。首先，你可以对业务流程生态系统进行评估，以明确你将考虑从外部供应商处采购的具体流程，以及这样做的利弊。

作为评估的一个关键环节，你需要衡量当前流程对短期和长期业务战略的价值，以及有待改进的地方。另外，请记住，快速发展的云能力可能会带来新的商业模式和开箱即用的可能性。当公司开始外包无法提供具有竞争优势的 IT 功能和业务流程后，他们便能将精力和投资转向有竞争优势的“差异化”系统和服务，同时实现可持续的变革能力。

不必通过为期两年的庞大项目来完成评估工作。事实上，可以一步一个脚印，逐步提升大部分流程的效率和效益。与此同时，你可以着手将人力和物力重新投入到能够带来竞争优势的差异化流程中。

从基础设施到行业垂直

目前推动云走向行业垂直化趋势的业务和技术需求并非是新的需求。从 2000 年开始，具有合规需求、业务流程处理需求或数据管理需求的组织开始采用云技术软件。大约在同一时期，许多企业的首席信息官开始将一些企业内部系统整体迁移到公有云上，以降低成本和提高效率。

今天，采用满足行业通用需求的共享软件和基础设施外包这两种相辅相成的方式， 共同推动着云走向行业垂直化的趋势。 目前最新的进展是，我们已经从通用功能和通用库的采购，转向与实际的行业业务流程数字化和可用性相关的工作。此外，越来越多的企业期望云计算供应商能够打造“通用核心”解决方案，满足各个行业和生态系统共同的需求。所以，云计算和软件供应商目前提供了具有行业属性、模块化业务流程的一个“菜单”，通过 API，只需一个按钮就能实现。例如，工程师和系统架构师可以使用 API 将特定的智能工厂系统连接到云共享网络中。如此精妙的能力与几年前的FedRAMP-esque、基于合规性性的产品相比有了质的飞跃。

在此背景下，我们看到这一趋势体现在以下几个方面：

超大规模云服务商向着堆栈上层方向发展

三大云服务提供商——亚马逊AWS 、谷歌云和 微软Azure——提供了基于云的行业飞地，使医疗、制造、汽车、零售和媒体等行业中特有的业务流程实现自动化。

他们先是创建了基础设施即服务 (IaaS) 能力，这些能力最终升级为平台即服务 (PaaS) 能力。

但他们并未止步于此。超大规模云服务商的业务继续向着技术堆栈更高层次延伸，有条不紊地将不断增长的订单流程自动化，搭建行业优化平台。在某些情况下，这些平台的功能比许多企业应用的现有解决方案更加可靠和高效。例如，现在酒店业中的一些企业会基于云技术的预订和客户管理系统。制造业也同样利用云技术的预测性维护解决方案。

各组织将能在行业云中发现超大规模云服务商开发的产品和服务以外的价值。可以肯定的是，MuleSoft、Oracle、Salesforce、SAP、SrevisNow 等知名供应商，以及初创企业和开源项目所提供的行业特定业务能力形成了生态系统，而且在不断发展。[6]

关注差异化

很有可能你有一些自行开发的代码/系统，你可以保留下去。得益于良好的规划和实施，你投入时间和预算所开发出这些能力能够为你带来竞争优势。你需要将它们视作能让你的组织在市场中脱颖而出的关键因素。 例如你是一名零售商，花费了大量时间定制你的店内库存管理引擎，而最高管理层 (和市场) 十分认可你的库存能力并且将它视作一流的超能力。云服务供应商能够提供库存 API 并不意味着你就应该不假思索直接使用它们提供的产品。既然你拥有定制化的能力，而且相应的能力对实现竞争差异化优势能起到关键作用，那为什么不考虑把它留着呢？当然，你可以在云端获得相应的能力，但重要的是你定制的系统你就拥有其知识产权，能够满足你独特的需求，而这是现成的产品无法做到的。

采取行动前，你必须对各项选择进行评估。目前聚焦垂直化的解决方案与前几年相比也更为复杂和精细。执行某个流程前应该考虑现有的能力。如果你当前的能力比供应商提供的能力更好，那么就该维持原本的运行逻辑。但是，如果你的竞争对手是“数字化原生”企业，而你的流程以及相应的支持能力已不具备优势，这种情况下便可以考虑使用行业API。

对于许多技术和业务领袖而言，要跟上云走向行业垂直化趋势则必须精打细算。各个领袖必须一起识别公司在市场中的优势，以及哪些技术能够助力公司取得胜利。例如，如果你通过非传统客户服务赢得胜利，则应该对相应的内部分析能力进行大量投资，这些能力能够带来竞争差异化优势，以及新的创新和创收机遇。一定要尽心经营这样的能力。 相比之下，无法帮助你在市场上展露锋芒的能力则都是商品，都是可以从云服务或软件供应商处获得的商业服务。

在探索云走向行业垂直化趋势的潜在机遇时，可以考虑展开以下行动，其中可能还包括一些早就应该采取的措施：

1. 业务和 IT 负责人应该展开合作，明确公司当前和未来的优势。要实现这一目标，业务负责人必须深化对技术的认识。同样，IT 负责人也必须了解业务战略以及技术在推动业务战略进展方面所扮演的重要角色。只有这

样，两个团队才能确定哪些技术是帮助公司赢得胜利的关键。

2. 制定业务流程以及支持相应流程的云产品清单。

3. 明确应在公司内部保留哪些差异化流程和技术。此外还需要判断业务范围内哪些领域能够从云技术赋能的新兴技术产品组合中获益。

4. 与云服务供应商、软件供应商和集成商合作，规划公司云能力发展的下一阶段。

现代工程

即使“购买”流程演变为“装配”流程，不同的“构建”方式也同样具有必要性。我们所讨论的并不是大批开发商为构建庞大的定制化系统而进行持续数年的项目。相反，我们讨论的是现代软件工程：小团队使用云服务、平台和工具开展工作，快速完成集成和部署。

这一新方法的很大一部分都是关于全栈团队围绕一系列明确界定的结果紧密合作。领导性质的组织接纳“小分队”或“双比萨团队”，其中云工程师、用户体验设计师、数据科学家、质控人员和产品经理会在工作中进行合作，各部门的边界因此变得不再绝对。团队成员更关注当前冲刺阶段的关键问题，他们也就能在这一过程中学习和成长。重要的是，团队会集中精力解决业务问题，针对正在开展的工作形成路线图。这意味着团队迎来了可喜的转变，从原先不明确方案要求的制定目的到如今有针对性地开展工作的变化。

另一个关键是赋权。现代工程师希望拥有自主权，包括从目的角度（可以选择做他们认为有意义的工作），到工具角度（可以选择他们用来施展技术的设备、平台、开源库），再到个人角度（着装要求、工作时间、远程办公安排）。

传统组织的技术领袖在访问高科技初创企业时，通常未能把关键的东西带给自己的组织。数字化原生企业的工程团队能够迅速发展的原因通常并不是因为他们有供员工娱乐的桌式足球、装满零食的冰箱或是一些没有意义的特殊福利，而是因为这些新型公司将工程视作极具创造性的核心领域。他们尊重工程师的意愿，并赋予工程师有助于他们取得成功的权力。当然，限制和指导方针依然有必要，尤其是涉及安全、合规性和法律知识产权保护等问题的情况下。不过这些都是将现代工程提升为组织战略和未来文化的一个关键部分的大背景下部署的。

培养持续变革的能力

在创新技术日新月异的时代背景下，获得一流的解决方案甚至是实验性的工具为企业提供了他们需要的软件选择，以连接他们多方面的数字转型战略的所有点。然而，这取决于组织是否具备适应变化的能力。

设想一下：随着创新解决方案和服务的出现，适应特定行业垂直需求的云技术将不断演变。
为维持自身竞争差异化优势，组织需要接受变化，保持应用最新的行业云产品。 由于变化极其迅速，未来总是会快速逼近。云技术不仅可以帮助组织实现变革，还能使组织拥有持续变革的敏捷性。如今内部的系统和流程越少，未来需要进行管理、升级和更新的任务也就越少。大多数公司在一定程度上都已在云端部署业务。如果你的公司也是如此，可以把行业云趋势看作是公司“云之旅”的下一阶段，它是对云计算最初承诺的再现，即共享资源，以节约成本和规模化的方式。

未来的方向

值得庆幸的是，要完全拥抱行业云趋势，企业无需耗费九牛二虎之力。事实上，只要采取小而周到的步骤，避开复杂遗留应用程序更新或颠覆性核心现代化方案的问题，就能实现你的目标。而你的每一步进展都有助于提高系统效率和效益。

中国分享

行业云：边界、机会、价值

在中国，随着经济高速发展和新兴技术的不断成熟，很多行业、企业加快了数字化转型的速度。

我们可以看到这样的趋势，制造、金融、贸易、医疗等很多行业具有优势与影响力的头部企业，突破了原有的内部优化，自我提升的局限性，转向了全局优化、行业赋能的数字化战略。这些企业会协同云厂商、专业咨询服务机构、软件服务商和系统集成商以云平台为技术底座，以数据湖、数据中台为数据底座，开发一系列基于云的带有行业特定属性的解决方案，形成面向垂直领域的行业云平台、行业一体化供应链平台、工业互联网平台、行业大数据中心等。

金融行业中规模大的银行或保险公司，利用自身技术上的沉淀与规模优势，将自身建设的集团云平台向行业全栈云升级，聚焦行业发展，输出行业核心能力，打造行业生态。金融行业云平台可实现行业PaaS、行业SaaS基于模板进行应用云化，同时支持多种集群架构，覆盖各类企业应用，帮助行业内中小企业解决上云痛点。

贸易行业中的领先企业进行数字化转型的过程中，在原有B2B互联网平台的基础上，融入了云原生、物联网、区块链、大数据技术，形成了新的行业服务模式，构建面向垂直领域的行业云，将打破行业内部的信息孤岛，通过数据驱动，带动资金流、商流、物资流、信息流，打造面向行业一体化的数字化新型能力体系，促进业务和技术一体化融合、深化产业链、供应链一体化协同、通过平台赋能行业快速发展。

从行业云的发展新趋势，我们可以看到有两个关键词，一是平台赋能、二是数据驱动。企业已经从过去的以流程自动化为中心、相对封闭的传统IT架构，完全转向了以能力复用和数据共享为中心、互联互通的“云平台+数据湖+服务化”的新型IT架构，我们可以称之为企业新一代数字基础设施。“应用上云、数据入湖”已经成为很多企业数字化转型的主要抓手。

以领先的制造行业云平台为例，除了底层云平台的IaaS、PaaS等基础服务外，还有很多具有行业属性与行业特点的业务能力和数据服务以数字模型、微服务组件、行业APP等形式面向行业提供能力共享、服务共享。其中，数字模型包括机理模型、业务流程模型、资产数据模型、数学算法模型、设计仿真模型等，通过行业云平台，在企业间建立互联互通机制，共享发布的数字模型，提升企业应用的开发效率。同时，也支持企业创建数字模型，参照行业发布的技术标准与业务规范，向行业申请发布模型，申请成功后，可由行业云平台统一管理并在全行业共享。

行业云的广泛应用，将全面提升行业应用和解决方案快速迭代创新能力，支撑行业内部产业链和上下游生态数据资源有序流动，促进资源动态优化配置，以数据流通促进科学决策、运营优化、业务创新，有效应对转型带来的不确定性。帮助企业在生态系统及价值链中构建与外部安全共享数据的能力，进而孵化新的商业模式和产品，为行业带来了更多的机会、为企业创造更大的价值。

我的观点

Marijan Nedic
SAP副总裁
兼IT业务解决方案负责人

我相信能够让你与竞争对手拉开距离的东西并非是你业务的主要部分，而是那 5%-10% 独一无二的业务。

行业云的出现——由特定垂直行业所使用的，整合了通用应用程序和配置的解决方案——正在帮助企业花更少的时间来设置经营业务所需的关键功能，从而有更多时间建立自身优势。SAP 的目标是创建行业云，是我们的客户能满足大多数开箱即用的需求，能与合作伙伴解决方案轻松集成，并且能在一个综合平台中管理独特的差异化产品。

无论你经营的是医院、工厂、汽车租赁公司还是其他领域的企业，你和竞争对手所采用许多流程和操作实际上都大同小异。因此，行业已经预先界定了你大部分的问题空间，而大部分的问题都已有解决办法。

因此，任何有着应用价值的行业云都会具有一些共同特征。首先，行业云必须提供行业所需的大部分开箱即用的功能，尤其是商品功能。第二，它必须是一个开放的平台，使客户和合作伙伴能够开发创新的解决方案。平台连接和管理这些解决方案的方式要便捷。第三，平台允许客户根据需求增加或缩减产能及流程。最后，平台要能方便地获得其它业务与技术服务。例如，今天所有主要的云服务都包含能够开箱即用的常用工具。虽然自然语言处理 (NLP) 已成为通用工具，但如何将其融入业务才是需要考虑的问题。行业云最重要的一个特征就是它需要能为更广泛的生态系统提供支持。

最近，我拜访了一家制造业客户，该企业该利用敏捷生产方法应对大大小小的客户订单。尽管业务利润十分可观，但却需要频繁地重新配置生产线。为了优化设备性能，他们利用机器学习 (ML) 模型分析订单数据，以确定必要的机器配置和履行订单的最佳顺序，该过程十分精密，但制造商的数字团队花费了大量精力才亲手构建出这样的模型。

实际上，这些能力通过单个行业云便能实现。将大部分构建和维护流程转移到云端可以为数据科学家留出更多时间开发机器学习模型，帮助工厂更快处理订单。如果将机器视觉与机器学习模型相结合，质控团队便可以检查更大比例的下线货物。比起亲自构建能力，将时间投入到真正重要的工作中，制造商也就可以更快提升业务规模。这些都是让制造商脱颖而出的重要因素。

有了相应的功能组合，企业可以变得更加敏捷。当其主要运营平台的配置采用的是所在行业的典型配置时，他们可以将精力集中到能够帮助他们实现独特优势的业务部分。可以直接将工作重心放在业务、合作伙伴网络、供应商网络以及设备的数字化内容上。最关键的一点是，必须足够敏捷，开发真正能够使你的组织与众不同的创新技术。

高管视角

战略

云服务供应商和软件供应商正不断开发日益复杂和强大的业务功能，并以服务模式对外呈现。拥有了更多外包机会，首席执行官就必须明确组织独有的价值主张。正如ERP将大多数后台功能标准化一样，领导者必须确定哪些子集的业务功能是差异化的。只不过现在赌注更大了：被取代的不是财务或会计部门，而是构成业务核心部分并影响着战略决策的部门。

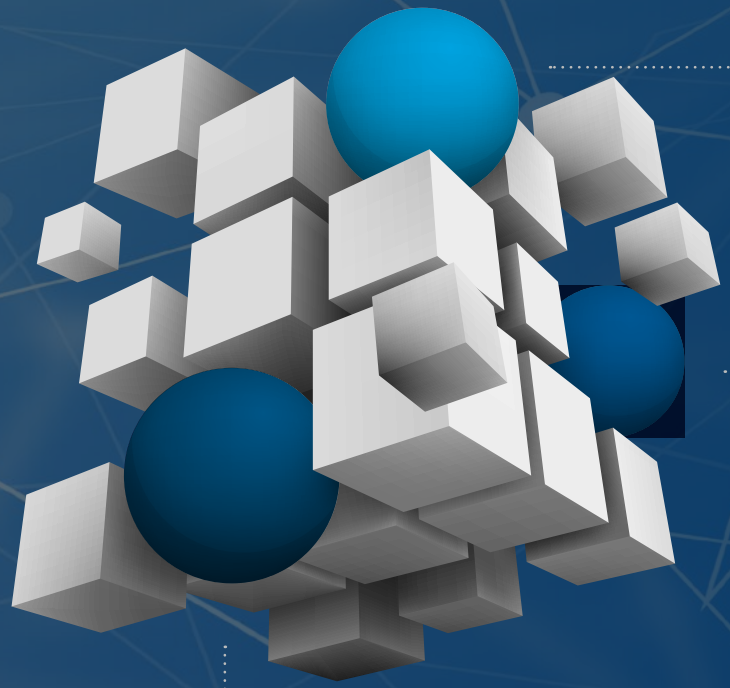
金融

对预算和合规要求感兴趣的首席财务官，可能会根据行业需求定制的、基于云的应用中挖掘出两重好处。行业云能够帮助企业以更少的投入跟上技术和监管变化的步伐，让人才留出更多精力去做增值项目。首席财务官需要确保财务、IT、合规、风险和法律职能部门密切合作，以使得各部门都清楚如何将新型云服务的潜在效益最大化。

风险

在新的行业云部署开始阶段，首席风险官有机会整合网络风险管理。供应商标准的网络安全组件可能无法满足组织的应用需求。随着行业云的发展带动着更多业务功能形成，定制化云安全的重要性也越发凸显。首席风险官和 IT部门可以使网络安全成为组织云技术堆栈的差异化因素，而不是等到以后再来考虑这一问题。尤其是面向消费者的组织，长远来看，从一开始就构建网络保护能力实际上可以节省更多成本。

你准备好了吗?



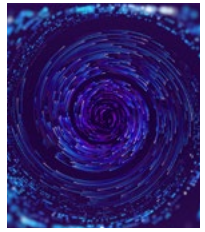
关键问题

1 目前有哪些你的组织与行业内其他企业都支持的非差异化流程? 你合作的供应商是否提供了更具成本效益的行业定制化解决方案?

2 未来几年, 哪些技术对你的成功至关重要? 如何将更多的财务和发展资源转移到这些领域? 你应该将它们保留在本地, 还是迁移到云端?

3 对于未来总是会“快速逼近”这一状况, 你是否已经做好了准备? 为创造和培养跨系统和跨流程的变革能力, 你可以对自己的数字化转型战略做出哪些改进?

了解更多



Reimagining digital transformation with industry clouds
了解如何借助行业云聚焦自身优势以充分利用转型战略。

Awakening architecture with cloud innovation core
了解相关组织如何凭借最新的云原生方案实现技术创新目标。

Deloitte on Cloud blog
重新思考云技术能为你的业务带来什么优势, 了解真实的洞察和专家看法。

作者

我们的洞察可以帮助你把握新兴趋势的机遇。如果你在寻找应对挑战的灵感，那我们可以谈一谈。

Ranjit Bawa

美国云技术负责人
德勤管理咨询
rbawa@deloitte.com

Brian Campbell

战略负责人
德勤管理咨询
briacampbell@deloitte.com

Mike Kavis

首席云架构师
德勤管理咨询
mkavis@deloitte.com

Nicholas Merizzi

云战略负责人
德勤管理咨询
nmerizzi@deloitte.com

资深撰稿人

Steve Rayment

合伙人
德勤澳大利亚

Benjamin Cler

高级经理
德勤卢森堡

Jorge Ervilha

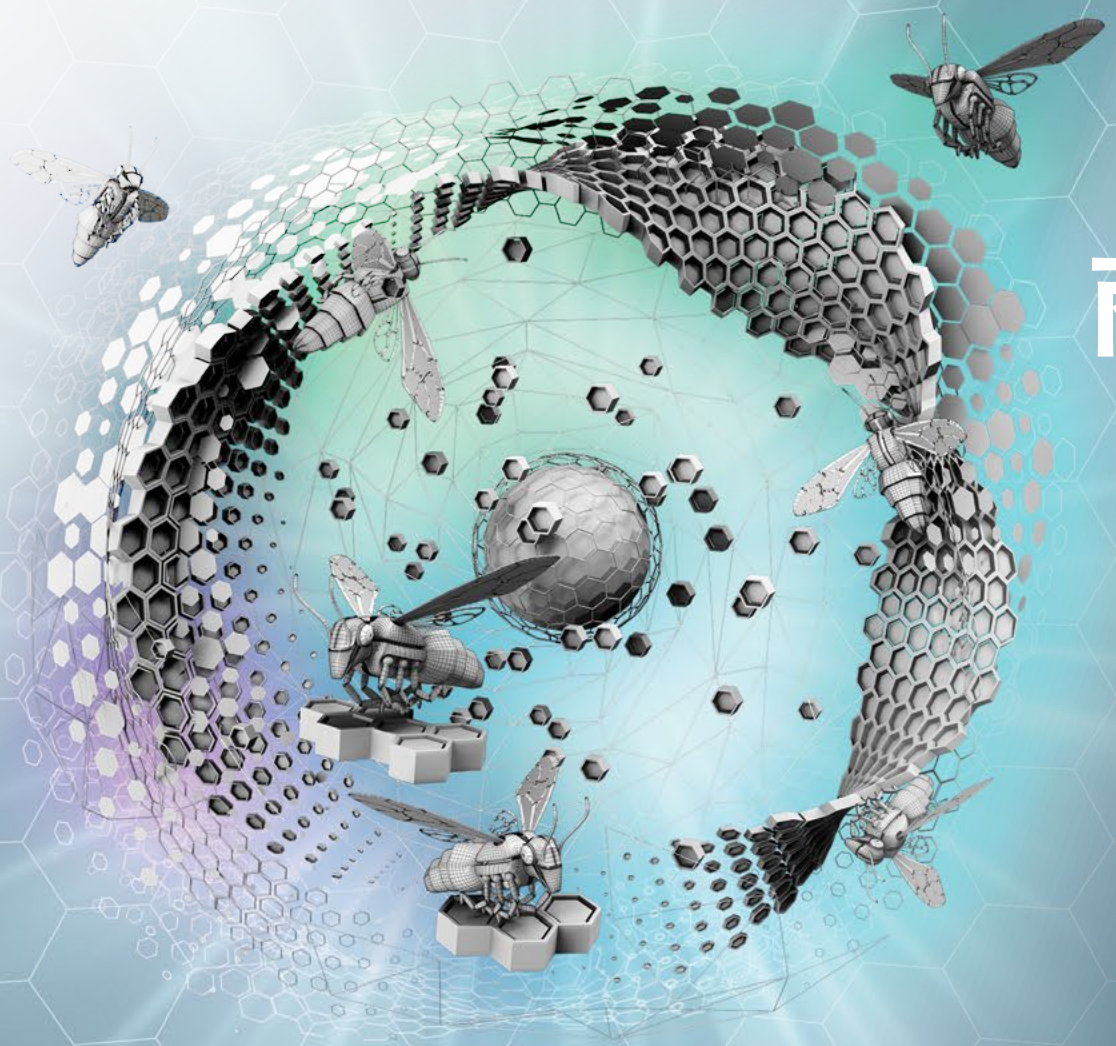
经理
Deloitte & Associados SROC, S.A.

Senthilkumar Paulchamy

经理
德勤管理咨询

尾注

1. According to the Flexera 2021 report *Cloud computing trends: 2021 state of the cloud report*, 90% of enterprises expect cloud usage to exceed prior plans due to COVID-19.
2. Kash Shaikh,"Industry clouds could be the next big thing," *VentureBeat*, March 28, 2021.
3. Ford Motor Company, Autonomic, and Amazon Web Services,"Ford Motor Company, Autonomic, and Amazon Web Services collaborate to advance vehicle connectivity and mobility experiences," April 23, 2019.
4. *Analytics Insight*,"HIPAA compliance, big data and the cloud—a guide for health care providers," September 15, 2021.
5. Brian Campbell, Nicholas Merizzi, Bob Hersch, Sean Wright, Diana Kearns-Matatlos, *Reimagining digital transformation with industry clouds: Organizations can leverage industry clouds to enable strategic transformation and stay on the cutting edge*, Deloitte Insights, November 23, 2021.
6. Bill Briggs, Stefan Kircher, and Mike Bechtel, *Open for business: How open source software is turbocharging digital transformation*, Deloitte Insights, September 17, 2019.



区块链：商业化应用启程

规模化区块链

成熟的技术、标准和交付模式促进企业的区块链技术应用。

金融业以外的应用

企业的区块链应用实践使得多个行业中涌现出区块链的创造性用途。

从需求出发

成熟企业和初创企业都必须以真实的需求为出发点，通过区块链实现商业利益。

趋势 3

区块链：商业化应用启程

分布式账本技术正改变业务经营性质，帮助公司重新设想如何管理有形资产及数字资产

新潮的加密数字货币和不可伪造的代币 (NFTs) 总是占据媒体头条，激发公众想象。不过，这些技术和其他区块链和分布式账本技术 (DLTs) 也在企业中掀起波澜。与为企业网络通信提供基础支持的 TCP/IP 协议一样，分布式账本最终可能成为企业运营的一个必要基础 (无形资产的情况下)，即使是看不见的基础，也能让既有行业领袖扩大投资组合，创造新的价值流，同时允许初创企业大胆构想振奋人心的新商业模式。

区块链和分布式账本技术平台已经成功跨过技术成熟度曲线的低谷期，目前正在拉动实际生产力。它们从根本上改变了跨越组织边界开展业务的性质，助力企业重新思考如何制造与管理身份、数据、品牌、渠道、专业认证、版权以及其他有形资产与数字资产。事实上，虽然许多公司在疫情期间取消了纯粹的投机性区块链项目，但是这些公司却加倍投资一些明显能够带来好处的项目。[1]

我们在先前的技术趋势报告中探讨过，标准化技术、流程和技能组合对扫除区块链技术应用及商业化过程中的障碍具有必要性。[2]今天，技术进步和监管标准 (尤其是在非公共网络和平台方面) 正带动金融服务行业以外的组织采用区块链技术。成熟的技术和平台通过提供互操作性、可扩展性和安全性来推动这一过程的进展。随着各企业越来越熟悉区块链和分布式账本技术平台，在许多行业中也涌现出一些创造性应用案例，并从根本上改变了跨越组织边界开展业务的性质。

规模化区块链：不断发展的技术和标准

第一代区块链和分布式账本技术已经证明了加密货币交易、清算和结算等应用方式行之有效，但同时也存在效率低、能耗大和无法规模化的问题。

首先，尽管市场中有着丰富的平台和协议，但却缺乏技术或流程标准以及互操作性，各个企业因此无法跨多个平台进行合作。早期的应用案例被限制在价值从一方到另一方的简单转移。用户无法创建能够使各方就条款内容达成一致的附带条件的交易或应急方案。

此外，技术的应用还受一些挑战的约束，这些挑战与交易验证相关。例如，加密货币和其他应用方式采用工作量证明共识机制来验证交易，这是一个十分复杂和漫长的计算过程，会消耗大量能源，每笔交易的服务费用很高，而且十分

耗时——每笔交易需花费 10 分钟或更长时间。[3]

这是大部分技术在早期应用阶段都会遇到的典型挑战，企业家、企业和学术机构因此开始推动区块链和其他分布式账本技术平台的产业化进程。如今，成熟的技术、不断发展的标准和全新的交付模式正吸引着更多企业拥抱区块链。比如：

非公共网络和权限网络。许多早期分布式账本技术平台都是低信任度公共网络，任何人都可以参与其中。这就导致网络中通常会有心怀叵测的人，而且这类网络也通常缺乏完善的隐私和匿名保护措施。现在，风险厌恶型企业拥有了更加可信和安全的选择：只允许通过筛选和验证的成员加入的非公共网络（即私人网络），以及通过身份验证的人可以加入许可（permissioned）网络（该网络中成员活动受限于相应的角色权限）。

技术进步。人们对可用性和速度的重视程度不断提高，导致第一代应用技术可能无法支持一些实际需求，包括设置自动执行合同和应急方案的能力。用于验证交易的新型加密流程耗能远低于工作量证明（proof-of-work，PoW）过程，而且突破了瓶颈，交易速度更快，每笔交易的服务费用和能耗也更低。在许多企业青睐的私有和许可网络中，授权证明共识机制被用来验证交易。

互操作性提升。许多满足企业应用目标的分布式账本技术平台不断涌现。Polkadot、Cosmos、Wanchain 以及其他新的协议和平台使企业能够连接多个区块链，并在多个平台上与多个实体无缝进行互动、协作、共享和交易。组织因此得以开发支持多种用例和个性化应用的基础设施。架构、共识机制、令牌类型和其他特征会因平台而异，组织可能需要根据具体的目标和用途探索更多平台。

技术和创新生态系统。随着分布式账本技术平台数量的增加，创新技术同步发展，一个广泛的、充满活力的生态系统已经出现了。其参与者正在开发去中心化应用程序，提供身份管理和供应链管理等专业功能。

如今，成熟的技术、不断发展的标准和全新的交付模式正吸引着更多企业采用相应的技术平台。

金融业以外的区块链

受更安全、更高效的交易效果吸引，金融服务业在区块链和其他分布式账本技术平台的应用方面一直处于领先地位。[4]但区块链技术所带来的好处也延伸至金融业以外的领域，尤其是在多个组织需要访问和共享相同的数据并需查看交易历史的应用场景中。一般而言，这是一个昂贵、低效且缺乏可信度和安全性的过程。但随着区块链和其他分布式账本技术的潜力在提高业务运营效率和创造新的价值交付方式层面不断凸显，金融行业之外的一些具有前瞻性的公司也开始应用这类技术，并将其整合到现有的基础设施和路线图中。

事实上，根据2021 年德勤管理咨询全球区块链调查报告的数据，绝大多数调查对象（80%）认为区块链、数字资产和/或加密货币解决方案将为他们的行业带来新的收入来源。[5]据另一家研究公司预测，全球在区块链领域的支出将从2021年的53亿美元增加到2026年的340亿美元。[6] 另有分析显示，银行业在区块链应用方面保持领先，其次是电信、媒体和娱乐行业；制造业；医疗保健和生命科学；零售和消费品行业；以及政府。预计从现在到 2024 年这段时间内，零售和消费品行业在区块链应用支出方面将达到最快的增长速度。[7]

备受关注的应用领域包括：

自主数据 (Self-sovereign data) 和数字个人身份。利用区块链和其他分布式账本技术平台实现安全存储和管理，用户便能建立个人数据所有权，创建和控制属于自己的防篡改数字身份。这有利于增强个人可识别信息的安全性，防止伪造或窃取身份信息的行为。具体应用包括联系人追踪、电子健康档案和电子证书以及电子表决。

第三方可信数据共享。就像在《数据跨界共享更便捷》中所讨论的一样，由于技术孤岛和隐私顾虑，第三方的数据访问和数据共享常常会受到限制。私有和许可分布式账本技术平台使组织能够安全地使用和交换数据，确保经验证和可信赖的第三方只持有必要的特定数据访问权限。在不牺牲数据完整性或数据隐私的情况下，组织可以跨公司和跨行业共享数据，促进生态系统伙伴间的协作和信任。例如，医疗保健服务供应商之间进行安全数据共享有利于改善患者健康信息的交流；在情报届，它可以促进跨机构和国际边界的威胁情报和其他可操作信息的交流。

资助。无论是对资助方还是受助方而言，区块链和其他分布式账本技术平台都可以帮助他们减轻与监测和报告财务及绩效结果有关的行政负担。一项针对联邦机构行动计划开展的研究发现，使用区块链进行、跟踪和监控专项拨款，提高了拨款情况汇报的质量和透明度，并且提高了拨付效率和汇报效率。[8]

公司间账务处理。特别是对于大型全球化组织或拥有众多法人实体的组织而言，公司间的清算和结算往往涉及多个企业资源规划系统、电子数据表和人工处理流程。此外，交易完成之后，对账工作经常会延迟数周。区块链和其他分布式账本技术平台可通过验证和创建一个共享的、不可变的转账记录，提升公司间 (尤其是在并购和收购过程中) 转账会计事务处理工作的可追溯性、透明度和可审计性。

供应链透明化。在当今的全球供应链中，利用区块链和其他分布式账本技术平台，可以优化产品跟踪流程并改善产品可追溯性，从而减少假冒产品，降低添加使用非法或劣质成分和组件的可能性；确保火鸡肉、钻石和葡萄酒等商品的货源正宗；并帮助政府有效施行关税和贸易政策。此外，采用上述技术也有助于进行资产跟踪、掌握货运情况，提高从采购订单和物流管理再到开具发票和付款整个采购流程的透明度。

客户和粉丝参与。将非同质化代币 (NFTs) 作为收藏品出售，使个人和组织能够构建数字社区、吸引粉丝和客户并打造自己的品牌。受新冠肺炎疫情影响，多地暂停举办线下体育赛事及娱乐活动，在此期间，非同质化代币帮助演艺人员和体育名人、相关行业从业团队乃至联盟实现了收入多元化，并与其粉丝和客户保持联系.[9]而在活动票务领域，应用区块链和非同质化代币具有彻底杜绝票务欺诈和 “黄牛” 倒票行为的潜力。

帮助创作者变现。艺术家、作家、发明家和其他创作者往往要花费很大功夫去通过许可使用、专利和版权，来证明自己对IP (智力创造成果) 的所有权，以及实现IP货币化。而借助区块链和其他分布式账本技术平台，内容创作者可以将其IP嵌入一种智能合约，每当有人下载这类IP，都会执行该合约。该智能合约可以触发自动付款，并能根据用户身份进行灵活处理，例如，大型企业将比个人消费者支付更多费用。

以业务和客户需求为导向

我们可以将当今的分布式账本技术平台与20世纪90年代中期的互联网进行类比，重点看一看互联网给各行业和生态系统的业务流程带来的变化。

回顾一下，在其尚处于起步阶段时，互联网速度慢、用户界面不够美观并且不为人所理解。一些传统公司没把它放在眼里——毕竟据他们推断，无论是网购还是电影流媒体，通通没有市场。而另一方面，许多初创企业满腔热情地加入了这一行列，在它们的企业名称中加入后缀 “.com”，并斥巨资经营业务、进行产品发布。

最终，双方的结局大都很糟糕。那些传统巨头中虽然不乏因为忽视互联网而被淘汰出局，但确有一些富有远见的老牌企业坚持到了今天，并最终成为互联网巨头。那些互联网初创企业中，如果所奉行的商业模式不具可持续性或存在缺陷，也都纷纷“阵亡”，但那些采取了可靠商业战略并具有执行力的企业却获得了巨大成功。当 .com 时代尘埃落定，留下来的是那些围绕有形业务和客户需求构建或重构其商业模式的公司。

区块链和其他分布式账本技术平台的现状与1997年的互联网并没有什么不同之处：他们不够灵敏、用户界面不完善，但在企业应用方面却存在无限可能。就像互联网一样，它们正在帮助企业和组织简化业务流程和运营，并通过创造新的数字商业模式来推动价值的实现。它们不需要使用传统媒介就能在组织边界之外建立信任，这种能力深刻地改变了创造和交付价值的方式，而且，就像互联网一样，它们正在改变跨行业和生态系统开展业务的方式。在单一组织内部，实施变革可能具有挑战性，而在多个组织和行业中，难度可能会上升好几个台阶。随着使用分布式账本技术的门槛降低，以业务和客户需求为导向的老牌企业和初创企业都能够更顺利地驾驭这一转型。

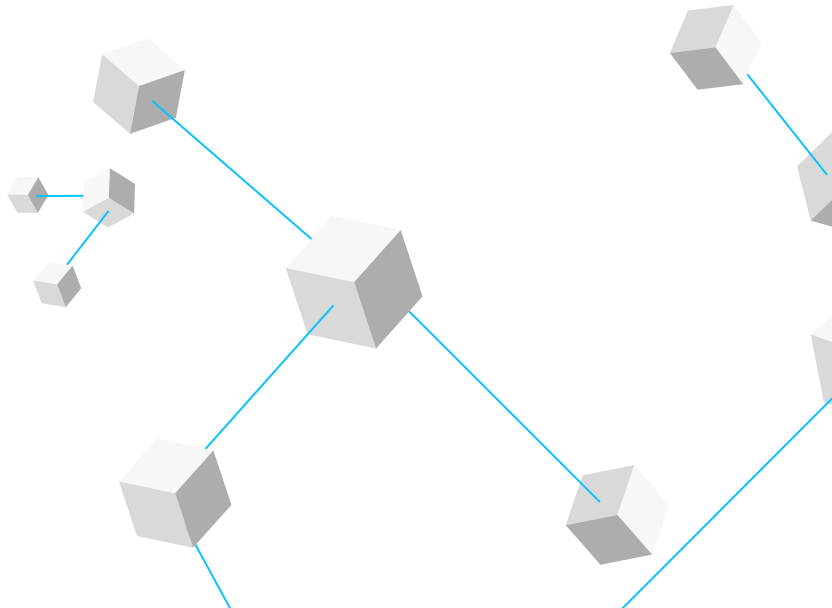
许多企业家和初创企业正致力于发现新的客户使用案例，并为基于区块链与其他分布式账本技术的新商业模式吸引投资者。例如，初创企业创造了基于分布式账本的作者身份验证方式，享有所有权的平台可以解决艺术家、作家和音乐家所面临的版权、归属、权限管理和版税支付等方面的挑战。ii但是，当这些技术试图颠覆其所在行业之时，既有的市场领导者并没有坐以待毙。相反，他们正在接受分布式账本技术驱动的商业模式，同时充分利用他们作为可信赖供应商的声誉。例如，微软依靠区块链为其游戏业务合作伙伴提供版税协议和付款记录。[11]

未来的方向

今天，成熟的技术、不断发展的标准和新的交付模式正在推动企业对区块链和其他分布式账本技术平台的采用。大量企业用例不断涌现，赋予了各行各业的组织开发新商业模式的能力，以改变各种形式的物理和数字资产的价值创造，并简化跨组织边界的业务流程。随着人们对分布式账本的信心不断增强，有朝一日，区块链上形成的集体记录会不会被视作比链下记录更可信的事情呢？

创新的商业模式可以帮助初创企业开辟新天地，并使传统企业有能力发展和补充现有的商业战略，从而在“无信任”的分布式账本生态系统中维持自己作为可信赖代理人的声誉。要想取得成功，无论是新来者还是老前辈，首先要做的可能都是确定客户或业务需求是否正当合法。

当组织利用区块链和其他分布式账本技术平台来推动创造新的商业价值，他们很可能需要了解哪些平台和协议与其所在行业和用例相关度最高，并对现有企业架构进行未来验证，以便实现在多个平台上运行。最后，为了支持这些技术和平台将带来的跨组织和行业转型，组织可以在改进或改变业务流程方面培养一种紧迫感，同时提升变革管理能力。



先行者经验

法国公共金融机构（Caisse des Dépôts et Consignations，CDC）扩大了法国金融业的区块链项目规模

法国公共金融机构已制定数项成熟的区块链发展行动计划。当许多公司尚处于试图弄清楚区块链究竟是什么，以及可能有什么用时，这个拥有 205 年历史的组织正在利用区块链解锁新的机遇，创造新的运营方式。

但这并不是一蹴而就的。当法国公共金融机构的区块链和加密资产项目负责人 Nadia Filali在2015年第一次听闻比特币以及支持这种加密货币的安全协议时，她意识到这是一个机会，但她也明白，这需要拥有一支具备多种专业知识的团队，以及一个广泛的合作伙伴生态系统。Filali说：“你不可能独自开展区块链方面的工作，合作是必然选择。”[12]

在与其他几家金融机构和区块链初创企业进行交流后，法国公共金融机构与其他10家组织合作推出了LaBChain，这是一个致力于探索如何利用分布式账本技术，为金融服务业发掘机会的联盟。当全体成员通过培训和实验对技术有了共同的理解，LaBChain使他们能够针对抵押品管理、共享客户详细信息 (KYC) 和欧元代币化等用例开发概念验证项目。现在，包括监管和研究者在内，LaBChain 拥有超过 35 位成员，已成为进入法国区块链生态系统的门户。菲拉利表示：“关键是要打造一个实践推动顾问团队，而不仅仅是一个智囊团。”

如果说该区块链和加密资产项目的一个使命是支持技术的采用，另一项使命就是为其业务部门和客户探索应用前景。Filali召集来自法务、IT 及财务部门的人员，组建了一支了解区块链及其潜在影响的内部团队，并开始实施各种解决方案。她的团队及其延伸出去的工作网络现在已有能力开发内部区块链产品，与监管机构就相关问题进行协商，并指导其他公共机构采用区块链。他们所做工作促成了与欧盟区块链观察站和论坛的合作。Filali 自2021年4 月起担任国际可信区块链应用协会 (INATBA) 的董事会主席。

Filali的团队还在开展一个与数字身份相关的涉及范围更广的项目。法国公共金融机构联合法国邮政，以及两家能源公司成立了一家名为Archipels的初创公司，专门提供文件认证服务。能源供应商可以在 Archipels 的区块链中提交其经过认证账单的哈希值（存在证明）。如此一来，银行或管理机构能够核实其客户提供的文件，减少欺诈行为。Archipels 目前拥有2000多万文件哈希值，在其分布式账本中创建并更新条目。Filali预计，有了第一项服务，更多类型的身份验证服务将应运而生，例如数字钱包。

而每一项举措的落实都需要 法国公共金融机构与法国政府各部门、商业协会和银行之间的通力配合与协作。Filali 表示，任何大规模区块链项目都有可能与这些机构互动，基于共同的热切期望建立一个合作伙伴联盟至关重要。她指出：“得到最高管理层的支持对我们的成长非常重要。”

随着区块链日趋成熟，建立这种伙伴关系可能会越来越容易。2019年和2021年，法国议会通过了一系列加密货币法规。这些法规要求加密服务公司向金融监管机构登记备案并遵守反洗钱和KYC (Know Your Customer，了解你的客户) 规则，以及其他义务。Filali表示，从某个角度来看，此举使加密货币和区块链具有了更大的合法性。现在，以往持怀疑态度的机构正在寻找这些数字资产接触的途径，并探索代币化和自主身份识别方面的具体用例。

“这就像行星排列一样。” Filali说，“我们有能量，我们有能力。而且人们都已明白，如果现在不采取行动，可能会错失良机。”

区块链对于一家珠宝集团的长期意义

总部位于中国香港的珠宝集团周大福是全球最大的钻石销售商之一。从所界定的业务范围来看，该公司购买和销售实物资产，但这并不意味着它不能利用新兴的数字工具。该公司目前运营数字销售和营销平台，分析客户数据，并实现了其大部分生产线的自动化。现在，它正在将区块链加入其数字投资组合。

周大福产品的主要价值主张之一是，其销售的钻石均有美国宝石学院 (GIA) 鉴定证书，并符合联合国金伯利进程的要求，该进程制定了针对钻石的道德采购准则。问题在于，在坚守道德准则方面表现不佳的卖家经常会绕过这些标准行事，从而以更低的价格出售钻石，而消费者很难分辨出其中的差异。

这就是促使周大福要创建一个区块链，将其所有钻石的认证信息数字化的原因。在对每颗钻石进行切割和抛光后，珠宝商会采用激光技术在钻石上标刻一个序列号，该序列号引用了由周大福和 GIA 共同维护的两方共享区块链分类账中的特定条目。通过这种手段可以长久保留关于钻石最重要信息 (包括原产地和等级) 的不可变数字记录。客户可以把钻石带到珠宝商那里，让他们查询序列号和相关记录，然后通过专用的移动应用程序访问该记录。

周大福珠宝集团商业分析和科技应用总经理李天熹 (Jade) 说：“我们就是通过这种方式来保护顾客。借助区块链，他们可以全面并彻底地了解自己购买的钻石有何来历、品质如何。” [13]

将这些信息放到区块链中也有助于周大福管理自己的内部流程。该公司旗下有5000多家独立珠宝店，其中约65%由加盟商拥有和经营。这些店铺每年总共加工约50万颗钻石，其中大多数 0.3 克拉或以上的钻石都有自己的证书。将经这些店铺流通的每一颗钻石与其证书一一匹配，这曾经是一个比较困难的过程。而现在，流程大大简化，只需将钻石上的序列号与区块链分类账条目匹配即可。

周大福正在寻求方法扩大其对区块链的使用范围，以期简化金融交易。加盟商有时需要向银行申请融资来支付购买存货的费用，而银行在提供信贷融资之前需要查看店铺的销售数据、收入水平和其他业绩因素相关信息。周大福目前正在研究如何将加盟商的数据录入区块链分类账本，从而加快流程并帮助加盟店在需要时获取所需的库存商品。

李天熹说：“我们的目标是使用区块链来存储这类业绩信息，方便银行进行验证。我们希望这能帮助加盟商更有效率地开展运营工作。” [14]

钻石是一种流动性极差的资产。它们具有可观的价值，但与现金或股票等资产相比，可能更难购买、出售和交易。但李天熹表示，针对钻石的价值创建数字记录将有助于减少这些方面存在的挑战。此外，这也有利于吸引年轻一代的买家，他们更有可能信任数字认证。满足这一更年轻、更了解数字技术的客户群的期望是公司需优先处理的关键任务之一。

李天熹说：“尽管周大福是一家拥有 92 年历史的公司，并且我们所在行业的历史更为悠久，但利用区块链等技术来把握新兴机遇是很重要的。我们是一家老牌公司，但数十年来，我们革新的脚步从未停止。”

在美国财政部，区块链如何从神秘变成主流

美国联邦政府致力于掌握其支出的每一块钱的流向，在这方面所下功夫远超大多数典型企业。在处理纳税人的钱时，透明度和问责制至关重要。出于这个原因，美国财政部正在研究如何利用区块链来实现自动化程度更高的新一代记录保存流程。每年，各联邦机构都会发出数十亿美元的拨款。这些补助金的接受方往往会使用这些资金向规模更小的次级受助方提供补助。每一分钱都必须受到追踪，其在每个组织的经手情况都必须掌握。根据历史经验，这意味着补助金接受方需要进行大量的报告和文书工作。

为了减轻一些负担，美国财政部的财政局正致力于开发一项区块链解决方案，以简化发放补助金和追踪资金流向的流程。该项目本质上是将补助金支付款项转化为代表实际货币的数字代币。接受方可以通过政府机构将代币兑换成现金，或将其拆分后分发给次级受助方，后者也能将其获得的代币兑换成实际货币。在此过程中，每进行一笔代币交易都将更新区块链账本，记录下有关转账金额以及转账目的的信息。

其中大部分信息是自动生成的，这意味着该过程将取代补助金接受方和次级受助方在获得政府资助时必须进行的大量汇报工作。一些评估报告指出，研究机构花在处理报告等行政工作上的时间超过了其总工作时长的44%。使用区块链来追踪款项流向后，这种情况将大有好转。

美国财政部创新项目经理Craig Fischer说：“我们能够将拨款的因素与所有这些资助信息对应起来.[15]我们知道资金来源、用途以及拨款的目的。完整的历史记录被铭刻于区块链上。使用区块链，进行记录的同时就是在进行汇报。”

该项目仍处于概念验证 (POC) 阶段。目前，该应用程序可以代币化补助金并将补助金和拆分后的补助金录入区块链分类账。需要做的最后一步是：创建一个将区块链账本与传统下游拨款系统连接起来的通用 API。

补助金拨付项目建立在已经由 Fischer 及其团队投入运行的其他区块链POC项目基础上。第一个项目是利用区块链来跟踪员工使用的手机。第二个项目旨在管理软件许可证，跟踪哪些员工仍在积极使用许可证，哪些许可证可以重新配置。

Fischer 说，这些举措中的每一项都是为了提升区块链在部门内的影响力，并证明除了加密货币之外，还有更多区块链用例。在政府机构中使用区块链面临着几个挑战。首要挑战在于，Fischer 表示他并不知道联邦政府内部有任何其他成熟的区块链支付项目，因此他的团队必须设计和开发访问控制和安全标准等配套流程。

但 Fischer 确信，他们的POC正在形成一股真正的吸引力，拉动整个联邦政府使用区块链技术。在最初阶段，最大的难关是让人们了解什么是区块链。现在，越来越多的人掌握了相关知识，他可以专注于展示区块链的价值。

Fischer 说：“过去必须要强调‘我正在用区块链来解决这个问题’，现在只需要说‘我正在解决这个问题’。”

中国分享

配合国家战略的区块链技术

2021年，国家“十四五”规划将区块链纳入数字产业。作为国家数字经济发展的重要一部分，区块链技术成为国家发展战略的重点之一并且在政府高层会议中多次被提及。

根据中国信通院的区块链发展白皮书，工信部和网信办也曾指出，要聚力解决制约技术应用和产业发展的关键问题，进一步夯实我国区块链发展基础，加快技术应用规模化，建设具有世界先进水平的区块链产业生态体系，实现跨越发展。区块链技术进入工程化发展期，向多层次融合创新、业务驱动优化演变。区块链基础功能架构已趋于稳定，面向业务场景需求的工程技术优化成为业界共识。以实现“高效、安全、便捷”的发展目标。与其他一些国家关注“元宇宙”概念的发展不同，中国区块链在过去一年来的发展表现突出，在政府的引导下，更加关注底层核心技术以及技术与再工业化产业需求的结合。

大力发展实体经济是我国的战略重点，区块链作为新一代的数字化技术，与实体经济加速融合，支撑国家一带一路、人民币国际化，全面提升国际影响力也是我国大力发展区块链的使命。配合国家战略，不断完善我国经济结构，提高政策落实和监管效率，夯实核心技术“短板”，在疫情新形势下确保经济继续稳中向好，加快物联网以及工业4.0，加强环境保护和如期达到“碳中和”目标等等，区块链技术无疑将做出巨大贡献。发展趋势上，区块链产业逐渐形成生态化的格局。

区块链作为数字经济的重要一环，将在跨产业联通，构建多方协作的可信任网络，对抗国际单边主义，加强国际协作，引领新一轮产业融合以及“全球化”扮演破冰锤的角色。

区块链技术垂直革新

从总体上看，区块链目前的技术和架构发展趋于稳定，区块链的核心技术包含共识机制、密码算法、点对点网络、智能合约、数据存储等等，而这些核心技术的革新和发展进展逐渐趋缓，在过去一两年革命性的技术相对较少而运维管理、网络安全、权限控制和跨链互通等等区块链生态扩展技术发展较快，且与其他信息技术融合趋势明显，行业焦点逐步由核心技术攻关转向为面向场景优化为主。

从技术发展上看，区块链技术发展重心开始从WEB3.0的技术革新开始转向围绕产业实际需求转移。从事区块链或分布式账本技术的相关企业或机构都开始进行垂直的区块链技术研发、技术安全、系统效率、平台化的便捷管理等细节需求成为了研发方向的重点。

公有链和联盟链在技术发展趋势上也有显著不同。过去一段时间，公有链在以太坊等开放性平台的带领下，逐渐地关注能效、环保以及安全。而联盟链等企业级应用这一类别，根据金融机构以及监管需求，则更加关注在节点管控、部署和扩展效率、性能安全以及监管合规性等等。

国内核心技术变革逐渐领先

中国作为区块链技术大规模应用的大力推动者，在过去一段时间对不少核心技术做出贡献，其中包括点对点技术革新、网络扩展技术、跨链互通技术、网络数据安全技术等等。

不少的区块链研发机构针对区块链的网络通行，提出不少点对点网络技术革新，持续加强节点通信能力，加大节点间数据传输协议，摸索更加高效的共识机制，这些不同的尝试和革新都很有可能成为引领下一代区块链实际落地场景的新标准。

“元宇宙”概念在全球区块链技术上成为新热点。随着NFT（非同质化货币）在行业里成为新明星，元宇宙的概念热点不断提升。元宇宙作为新的区块链发展方向，目前来看金融属性较为强烈。想要做出更大的实际突破，需要结合VR、AR以及人工智能物联网等科技的发展，更加需要一个可信任的、强有力的桥梁来链接虚拟世界以及现实世界。在元宇宙的初期，这些技术需求的思考和发展方向无疑带来更大的技术挑战。

区块链技术和实体经济结合应用

统计数据显示，中国目前从事区块链及其相关产业的企业已超过1400家，产业园区超过40个，专利申请数量在全球范围内也是非常可观，从整体上看，初步形成产业链条；区块链技术应用向供应链管理、数据流通、智能制造，数字货币、数字政府、金融证券等领域都有创新的落地场景。根据中国信息通信研究院统计，区块链在智慧农业、数据存证、疫情防控、冷链溯源等等的落地场景已经做出了不少的贡献。

除此之外，区块链技术作为整合数据共享平台，在结合物联网大数据、人工智能技术之下，打通实体经济与金融行业的信息壁垒，在供应链金融等方面也有广泛的应用。在供应链金融的场景下，国有银行包括建设银行等，也已经运用区块链技术进行再保理业务。再保理业务指的是以保理商为通道，供应商将核心企业为其担保的应收账款进行转让的一种融资模式，在这个模式下，需要企业配合银行进行合作，数据共享、数据鉴真等场景，通过保理商为其供应商提供短期融资。在我国对外贸易规模不断提升的背景下，再保理业务和贸易金融业务已经成为最常见的银行业务模式之一。然而这个场景现存在几个痛点：首先是银行与企业财务系统对接困难，区块链的易扩展性很好的解决了这个问题，并且能对数据和账目的真实性进行实时认证。二是解决异地客户业务流程繁琐的问题，异地客户可以很容易的远程电子KYC，开立融资户口，解决融资问题。

应用领域	发起机构	应用名称	覆盖区域
公共预警	山大地纬	济南疫情防空平台	山东省济南市
	链飞科技	区块链疫情监测平台	全国
物品溯源	蚂蚁集团City Do	疫情物资信息服务平台	浙江省
	北京微芯研究院	北京冷链溯源平台	北京市、浙江省、广东省等
身份互认	微众银行	粤康码	广东省
	纸贵科技	个人健康信息登记平台	陕西省西安市

来源：中国信息通信研究院

数字货币推动支付和芯片行业发展

中国内地的数字人民币成功落地应用，在2021年更是快速发展，带来了多款数字人民币相关的科技和产品。就目前而言，数字人民币主要针对M0以及零售支付，转账结算等场景，其推出将立足国内支付系统的现代化，充分满足公众日常支付需要，进一步提高零售支付系统效能，降低全社会零售支付成本。

目前， 中国内地已有超30家银行加入数字人民币体系。正逢2022年的北京冬奥会，数字人民币在奥运期间的零售场景更是吸引了不少参与者。据不完全统计，数字人民币的试点场景已经超过了350万个，数字人民币在不少商场、医院、学校、北京地铁、景区等均实现了数字人民币的结算。

在数字人民的广泛应用的推动下，央行通过数字人民币对国内经济良性发展情况有了更广泛的宏观和更垂直的微观的掌握。2021年数字人民币推出了革命性的双离线支付场景，使得收款方和付款方不使用网络的情况下仍然可以完成交易，但在这个场景下，对数字货币钱包安全芯片就有了更高的要求。

数字人民币的加快落地，促使紫光国微和华大电子等专注于国产安全芯片研发的公司都纷纷加入离线安全钱包的研发。数字钱包对数字安全芯片在电池续航能力，数据存储以及加密安全方面有极高的要求。数字人民币的落地应用要求相关芯片供应商必须提供更高的标准、更好的性能、更安全的防护，也促使国产供应商进行芯片研发产业升级，也为国产芯片的发展从需求侧注入更大的驱动力。

“百花齐放”到“生态融合”

区块链技术经过数年的飞速发展，在中国已经形成“百花齐放”的格局，各种区域性和小型的联盟链、协同链等层出不穷。但这又带来了另一个挑战，即在不同生态圈，区块链技术虽然都已经展开了应用，但是如何发挥区块链在数据互通、智慧启迪上的作用仍需探索。显然，生态之间的融合将成为未来区块链发展的主题之一。例如从单一的溯源场景到结合疫情联防联控，从数据存证到通过结合数字人民币和国家税务等将会给国家和社会发展带来重大变革的场景，仍然需要不同生态圈的互通互融，然而这一互通的驱动力在现时各自生态圈下未必很强烈。因此，政府和监管者将需要更加重视区块链的生态融合，推出更多的政策，以及利用市场手段来推动生态的发展。从“百花齐放”到“产业驱动”，“监管主导”将会是未来区块链发展的大趋势。

我的观点

Andre Luckow

博士，宝马
集团 IT 部新兴技术负责人

我已在新兴技术领域耕耘二十年，基于开展工作和研究积累的经验，我认识到了炒作和希望之间的区别，学会了辨别一项技术是否真正具有变革意义。

2018年，区块链正处于炒作周期顶峰，有人让我考虑一下，区块链有哪些潜在应用机会。自然地，我带着怀疑态度来看待这个话题。但随着我们的组织不断研究，我们最终找到了正确的转型用例。

我从数据的角度来看待业务问题，而对于宝马集团而言，多个运营项目需要更好的数据加以支持，其中之一就是我们复杂的供应链。我们在15个国家的31家工厂每天生产约10,000 辆汽车，我们的全球供应商网络庞大且复杂。而不久之前，我们还依赖于使用电子表格和电子邮件来开展工作。欺诈、对二级供应商的了解有限、供需不匹配都是可能导致生产中断、造成质量问题的常见问题。我的团队从一个概念验证项目入手，使宝马集团和少数供应商能够通过区块链以更容易地共享供应链数据。确保相关数据的实时可见性并对所有供应链成员开放，从而防止发生库存过剩和短缺问题。实现供应链透明化不仅让我们获得了更多关于配件来源的信息并由此受益，而且使我们的供应商能够发现改进机会。

在向领导层以及供应商伙伴展示了我们的原型之后，宝马集团看到了明确商机，因而投资以支持我们扩大区块链工作范围，以覆盖更多供应商。这项被正式命名为 PartChain 的行动计划实现了近乎无缝的透明化，并影响到了涉及范围更广的数据共享行动计划，例如 Catena-X、Automotive Network e.V.。Catena-X 在汽车价值链全线上创建了一个协作数据生态系统，使原始设备制造商、中小企业和回收公司等能够充分利用基于数据的安全经济的优势。从各方面来看，该技术已被证明在促进我们整个价值链的数据可见性方面是富有成效的。

我们也将目光转向改善驾驶体验方面，探索区块链在这个领域的用例。尽管在制造和供应链两方面我们已取得了一定的进步，但是，向消费者出售或出租汽车的流程却仍然麻烦重重，并会产生大量纸质文件。不久前，我们与德国政府合作，利用区块链将驾驶执照集中起来进行联合管理，并简化购车流程。实现自主身份识别后，德国公民能够时常联系共享汽车公司或保险公司验证其驾照，在最大程度上避免了冲突发生、保证了安全性，同时为卖家提供了一种简单方法来减少身份欺诈。我们期望，在不远的将来，购买一辆汽车可以像扫描二维码一样轻松简单。

回顾 2018 年围绕区块链的探索，以及宝马集团自那以来所取得的进展，有两件事是明确的。第一，区块链蕴含着变革力量，有朝一日，我们会在不知不觉中使用基于区块链的技术，因为它们有潜力打造更好的业务流程和客户体验。第二，实施变革所需的时间可能比任何人的预期都要长。企业要打开思路，思考哪些新的市场或生态系统可以通过区块链得到支持和简化。他们需要就数据驱动提出正确的问题，以找到适合于自己的用例。如果我们从各个方面推动技术向前发展，我们一定会看到更多伟大的想法浮出水面。

高管视角

战略

在区块链技术上，首席执行官们是有一种独特机会的：通过与他们的IT负责人合作，领略这类技术的无限可能性。当今在区块链技术领域所取得的进步类似于30 年前互联网采用TCP/IP协议的情况。尽管我们仍受到诸多限制，还无法全面、广泛地认识区块链技术，但其影响商业模式的可能性是巨大的。正如数据库使组织内部的业务流程得以重新设计，采用分布式账本技术可以简化组织之间的流程。首席执行官们需要决定多早开始采用分布式账本技术。

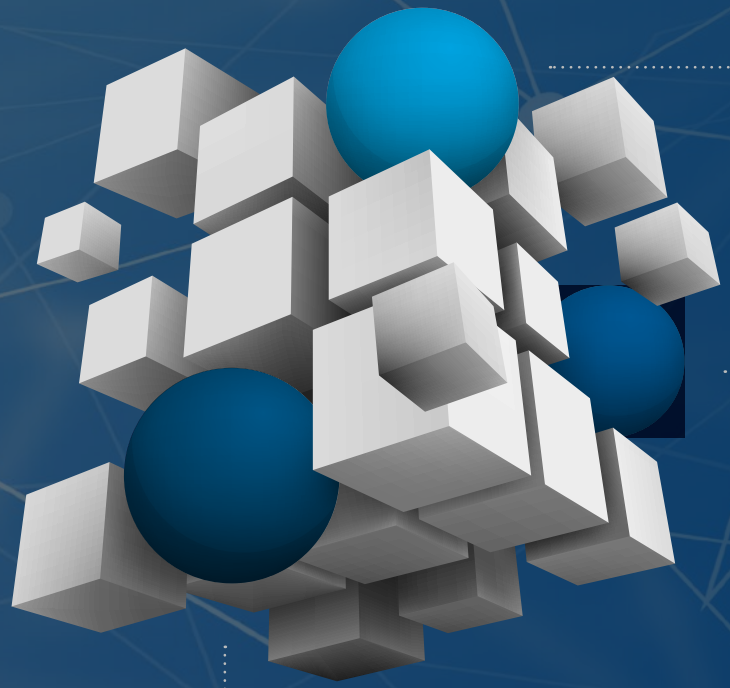
金融

尽管许多首席财务官已经承认区块链和其他数字分类账技术理论上具有效用，但涉及到全面采用时，他们往往无法下定决心。首席财务官可以使用敏捷技术来测试分布式账本技术用例，从而增强对其有效性和安全性的信心。他们可以与 IT 负责人密切合作，确定测试案例、部署实验并监测结果。一旦用例成功，组织就可以评审监管和财务方面的风险，然后扩大到企业内部乃至多方采用。

风险

企业对区块链的采用还不广泛，对该技术风险的理解仍处于初级阶段。首席风险官应与 IT 部门合作，以提高其组织在采用新兴技术方面的准备程度。他们可以制定技术采用路线图，确定区块链的用例，并积极主动地降低风险。例如，密码技术的新应用可以极大地提高交易验证的效率和可靠性，而基于区块链的数字身份解决方案可以加强敏感交易的安全性。此外，用于区块链准备的蓝图也可以应用于进一步采用新兴技术，如量子计算。

你准备好了么?



关键问题

1 通过充分发展区块链和分布式账本技术平台及标准可以解锁哪些新的交付模式、收益流或业务流程优化方法与工具?

2 去中心化将如何改进您与其他组织或生态系统合作伙伴的沟通、协作和数据交换方式?

3 您能否通过使用区块链来确保产品或服务开发、创造和分销的透明和可追溯性，从而发现建立客户信任或提升客户信任度的机会?

了解更多

2021 Global Blockchain Survey
查看最新见解，了解为何越来越多金融领袖将数字资产视为未来。

The rise of using cryptocurrency
思考使用加密货币和其他数字资产在投资、运营和交易方面带来的好处。

Blockchain to blockchains
看看多个区块链的协调和整合如何在整个价值链中共同发挥作用。

作者

我们的洞察可以帮助你把握新兴趋势的机遇。如果你在寻找应对挑战的灵感，那我们可以谈一谈。

Wendy Henry
政府与公共服务区块链负责人
德勤管理咨询
wehenry@deloitte.com

Linda Pawczuk
全球区块链与数字化资产负责人
德勤管理咨询
lpawczuk@deloitte.com

资深撰稿人

Hiroki Akahoshi
总监, Deloitte
Tohmatsu Consulting LLC

Marie-Line Ricard
合伙人
Deloitte France

Tyler Welmans
总监,
Deloitte MCS Limited

Claudina Castro Tanco
高级经理
Deloitte Consulting LLP

Jesus Pena Garcia
高级经理
Deloitte Luxembourg

Wiktor Niesiobędzki
专家领袖
Deloitte Poland

Ruchir Dalmia
高级顾问
Deloitte MCS Limited

Lily Pencheva
高级顾问
Deloitte MCS Limited

Nicklas Urban
高级顾问
Deloitte Consulting GmbH

尾注

1. Martha Bennett and Charlie Dai,"Predictions 2021: Blockchain," Forrester, October 28, 2020.
2. Deloitte Insights, *Blockchain to blockchains: Broad adoption and integration enter the realm of the possible—Tech Trends 2018*, December 5, 2017.
3. John Schmidt,"Bitcoin's energy usage, explained," *Forbes*, June 7, 2021.
4. KBV Research, *Global blockchain technology market by type (public, private and hybrid), by component (infrastructure & protocols, application & solution and middleware), by enterprise size (large enterprises and small & medium enterprises), by industry vertical (BFSI, IT & telecom, healthcare, retail & ecommerce, government & defense, media & entertainment, manufacturing and others), by regional outlook: Industry analysis report and forecast, 2021–2027*, May 2021.
5. Linda Pawczuk, Richard Walker, and Claudina Castro Tanco, *Deloitte's 2021 Global Blockchain Survey: A new age of digital assets*, Deloitte Insights, 2021.
6. Yahoo.com,"Global Blockchain Market (2021 to 2026) - by Component, Provider, Type, Organization Size, Deployment, Application, Industry and Geography," accessed November 29, 2021.
7. Fortunebusinessinsights.com,"Blockchain Market Size, Share & Covid-19 Impact Analysis, 2021-2028," accessed November 29, 2021.
8. MITRE, *Assessing the potential to improve grants management using blockchain technology*, 2019.
9. VISA, *NFTs: Engaging today's fans in crypto and commerce*, accessed November 2021.
10. 101 Blockchains,"Real world blockchain use cases—46 blockchain applications," July 6, 2018.
11. Rachel Wolfson,"Game time? Microsoft adopts Ethereum blockchain for gaming royalties," *Cointelegraph*, December 18, 2020.
12. Nadia Filali (head of the blockchain and cryptoassets program, Caisse des Dépôts), interview, October 15, 2021.
13. Jade Tin Hei Lee (general manager of business analytics and technology applications, Chow Tai Fook Jewellery Group), phone interview, September 23, 2021.
14. Ibid.
15. Craig Fischer (innovation program manager at the US Department of the Treasury), interview, October 29, 2021.

IT的自我颠覆：自动化技术的规模化应用

基础设施自动化	通过代码（而非人工）管理基础设施
系统和软件管理自动化	通过代码（而非人工）管理系统、工具和软件
自动化技术的优化	关键领域实现机器学习（识别可能的中断）

趋势 4

IT 的自我颠覆：自动化技术的规模化应用

那些着眼于未来的 IT 组织，已经开始对 “IT后台” 进行现代化改造，以形成具有前瞻性的自主服务和工程自动化模式

但还有许多组织内部仍然有员工在做着大量重复性工作，例如管理、监控、审查和工单响应等任务。过去十年，云服务供应商已经向我们证明了，剔除重复性工作的自动化流程，有助于提高整体效率。自动化流程具有一致性和可审计性，这有助于减少错误、提高质量。同时还可以让技术人员腾出双手，专注处理更高价值的任务。

由于各种原因，IT 领导者寻求自动化的步伐一直很慢。但是，这种情况开始发生改变。我们所观察到的一个新兴趋势是，某些首席信息官开始对其所在的组织和技术队伍进行了大刀阔斧的颠覆性变革，涉及的内容包括目前人工执行的大量任务，以及跨系统、架构、开发和部署的交接工作等。

除了利用云服务供应商的投资加快变革外，首席信息官还借鉴了云服务供应商的经验，识别各种流程并实现标准化。他们抓住基础设施、软件组件、安全和应用程序方面的各种机会。一旦改进措施成熟，首席信息官及其团队会利用人工智能和机器学习等先进技术，优化新的服务交付和自动化技术。除了利用云服务供应商的投资加快变革外，首席信息官还借鉴了云服务供应商的经验，识别各种流程并实现标准化。他们抓住基础设施、软件组件、安全和应用程序方面的各种机会。一旦改进措施成熟，首席信息官及其团队会利用人工智能和机器学习等先进技术，优化新的服务交付和自动化技术。

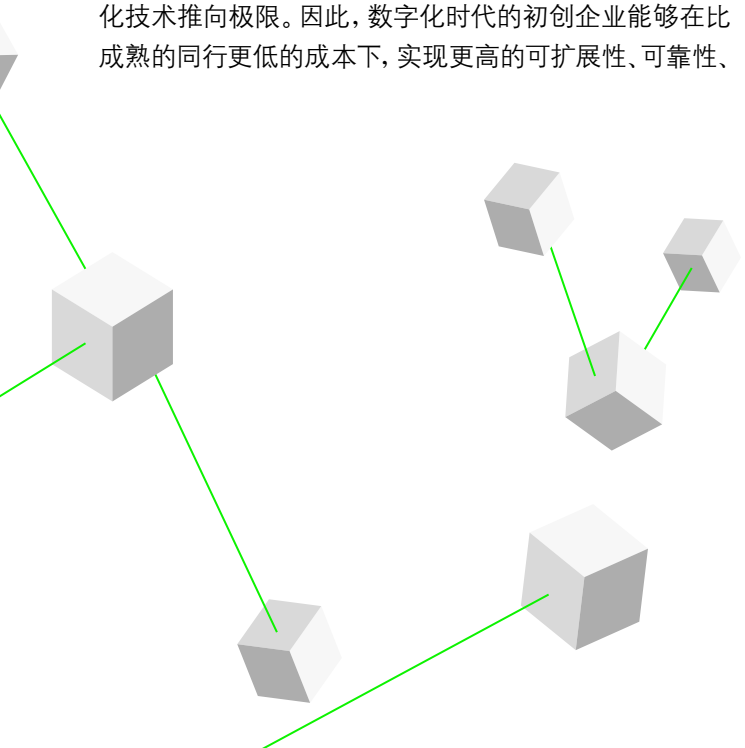
这一趋势下的早期参与者已经看到了效率的提高和劳动力成本的降低。在最近一项对 IT 和工程领导人的调查中，74%的受访者表示自动化帮助他们提高了劳动力效率。59%的受访者称团队采用流程自动化后降低了30%的成本。[1]除了显著提高质量和安全性以外，调查还明确了为何95%的受访者会将流程自动化置于优先位置，其中21%认为其应属于高度优先事项。[2]

变革的步伐只会继续加快。 企业想要获得更多，且希望比以前更快。人才市场趋于白热化，高技能人才的需求不断增长（永远供不应求）。大家都在努力尝试着以更少的代价获得更多的效益。

到了（最终）颠覆IT的时候了！

颠覆性的旅程

从人工到自动化的转变并不新鲜。 实际上，在过去的技术趋势报告中，我们已经在网络安全、高级网络和硬软件动态配置等领域研究了这种转变。那么，今年会有什么不同呢？简单地说，就是竞争。新冠疫情正在颠覆整个劳动力市场。也许，更重要的是，那些数字化 “原住民” 的DNA，将自动化技术推向极限。因此，数字化时代的初创企业能够在比成熟的同行更低的成本下，实现更高的可扩展性、可靠性、弹性和效率。他们还拥有一个额外优势，即他们没有被技术债务或组织妥协所拖累，而这些妥协需要交接和人工干预。对于数字化 “原住民”，这种老派的做法只能算作最后的手段，不是常态。这种方法与成熟组织经常采取的方法有根本的不同。如今竞争激烈的市场需要更强健的 IT 态势，这可以转化为竞争优势。



组织若想寻求契机颠覆现状，可以着重从以下三个方面入手：

企业内部基础设施标准化和自动化

自动化旅程的第一站是让代码控制所有基础设施和管理功能。对资源的程序化控制使其有可能一致地应用规则，并在自动化代码和配置文件中存储以前的手动配置。这些解决方案需要部署一些计算（容器、虚拟服务器和功能）、网络（软件定义的）和存储的组合。

为了使自动化规模化，流程必须在整个企业内一致执行。但是，从如今许多组织的运营状况来看，仍有一些流程、应用程序和方案还比较混乱。当进程在服务器A上以一种方式工作，而在服务器B上以另一种方式工作时；当环境不具有同等性时；或当网络采用不同的行为方式时，操作就会变得更加昂贵和低效。

如果你存在这些问题，你可以考虑创建一种标准、通用的方法，来开发、部署和维护你的方案和组件。云服务供应商很早就意识到，资源的程序化控制程度越高，就越容易将环境视为程序进行管理。如今许多 “基础设施即代（IaC）” 的平台都可以追溯到早期基于云的自动化计划。

随着组织不断探索 “基础设施即代码（IaC)”，他们逐渐认识到，他们还可以部署 “安全即代码 (SaC)” 或 “运营即代码（OaC)”，全部利用配置或代码文件实现控制。“即代码 (as-code)” 的目标是推动建立一个环境，在这个环境中，所有的东西，甚至是定制的系统，都能遵循一套优化的规则。只要规则落实到位，即使只有一名工程师也能够控制目前需要若干管理员才能处理的海量资源。 这样可以将基础设施团队解放出来，像云服务供应商一样工作：实现自动化，充分利用自动服务的优势，摆脱困境。[3]

组织利用自动化技术简化运营和管理时，还应重新审视其启动过程。过去，搭建基础设施涉及复杂的采购工作，并伴随着层层审批流程。如今，增加一个虚拟化实例可以不需要任何级别的事先审批。对遗留环境中有意义的类似交接和审批进行识别和自动化处理（或消除），有助于简化操作，提高开发人员的工作效率，实现更大程度的组织敏捷性。

如果有条不紊地从战略角度出发，自动化可以实现可观的规模化经济。此外，它还有以下好处：

- 准确率更高：员工不再对文件、查询结果和报表进行主观性地解释理解。
- 安全性更高、弹性更强：规则应用更一致。值得注意的是，目前一种新兴的“安全即代码 (SaC)”趋势势头正劲。
- 可靠性更高：通过代码修复的问题一般不会再次发生。

我们提醒那些采用了供应商“即代码 (as code)”服务的组织，请确保你已经整理了你的流程和操作，以获得这些能力的最大收益。否则，你可能还会在现代环境中重现现有的限制。

标准化和自动化软件、管理工具和应用程序

前沿 IT 组织已经不再人工管理基础设施了；如今，他们开发可以自动管理基础设施的代码，可以提高可扩展性、效率和一致性。这种方法同样适用于软件组件、管理工具和各种应用程序。 现代化 IT 组织则负责管理软件代码，而软件代码又管理着开发、维护、运营和安全等方面。最终，相比一系列手动配置方案，管理一条代码会容易得多。例如，通过基础设施即代码 (IaC)，我们可以将软件开发敏捷性引入基础设施管理中。从部署的角度看，人们可以实现全栈解决方案管理，不再由几个团队协调处理各个独立组件。

与基础设施一样，一些企业内部软件组件也可以实现自动化。 例如，数据库管理、集成工具、安全、系统管理和操作系统补丁等，这些都可以轻松被虚拟化和抽象化。

对于采用云服务基础设施的组织，供应商提供一个不断扩大的“平台即服务 (PaaS)”选项菜单，其特点是加强自动化、编程接口、集成中间件和管理能力。成熟的 PaaS 服务还可以提供增强的开发人员自助服务、编程接口，以及更紧密集成的中间件和管理能力。

如何决定从哪里开始？ 首先，确定那些试图向终端用户提供功能的“用户旅程”，以及这些用户会遇到的摩擦点。其次，果断去除不必要的审批和交接流程，然后为开发的代码和生产部署之间的步骤实现自动化或创建自助服务选项。最后，一旦启动自动化旅程，旧的性能指标可能不再适用。 为此，你需要定义适用于组织定位的指标，促进建立“自动化技术文化”。

利用机器学习和规则优化自动

自动化的第一关往往是基于规则的。 例如，“如果进程 x 未响应，重启进程”。随着时间推移，IT 人员可以像云服务供应商十年前展示的那样，识别出导致停机和故障的问题，并优化自动化工具来解决这些问题。最终，你可以超越基于规则的自动化技术，进化到基于机器学习的自动化技术。一开始尚不成熟的自动化旅程会逐渐朝着复杂化发展。自动化的第一关往往是基于规则的。 例如，“如果进程 x 未响应，重启进程”。随着时间推移，IT 人员可以像云服务供应商十年前展示的那样，识别出导致停机和故障的问题，并优化自动化工具来解决这些问题。最终，你可以超越基于规则的自动化技术，进化到基于机器学习的自动化技术。一开始尚不成熟的自动化旅程会逐渐朝着复杂化发展。

许多类型的机器学习，如预测、能力建模、行动响应、停机恢复等，都支持各种不同的 IT 活动。不过，对于大多数组织而言，机器学习的最优先事项是：及早识别停机，并利用预测建模来防止未来停机。通过关注这些领域，采用了机器学习的团队，可以显著提高正常运行时间，降低停机的严重性。此外，越来越多的 PaaS 产品具有嵌入式机器

学习功能。例如，PaaS服务往往利用机器学习，来维护和优化过去需要由开发人员、管理员和工程师手工管理的日常操作。这样做的效果是：开发和运营可在更高层次上运行。

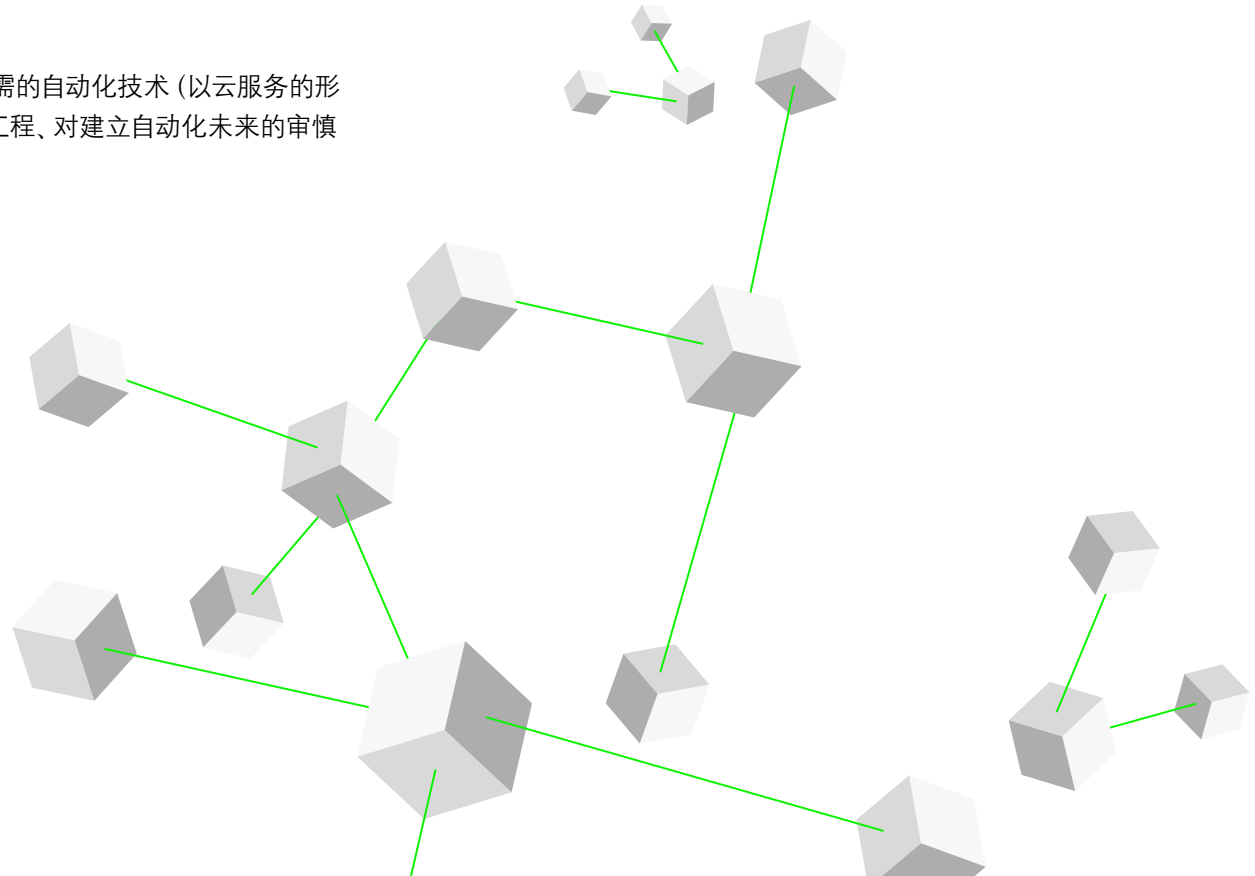
另一种优化技术涉及一致地应用规则。设想一下：企业架构是围绕“你可以使用什么”以及
“你如何使用”所做的一系列决策。而由此产生的规则代表的是架构设计和功能的最优方案。作为你自动化旅程的一部分，优先考虑一致性问题。在整个企业内，有条不紊地将规则融入各种系统和流程，可以实现这一要求。一致性带来最佳性能。

未来的方向

对于正在寻找自动化机会的首席信息官以和其他领导来说，时间是至关重要的。在如今急速发展的创新环境中，花钱雇人维护服务器和数据中心，并没有多大的商业价值。随着首席信息官利用自动化技术对其组织进行大刀阔斧的颠覆性变革，将有成熟的契机把员工的注意力从打补丁、监控和测量转移到更高价值的工程活动上。自动化技术可以广泛地延伸到开发、部署、维护和安全等领域，从而有可能提升更多 IT 运营的效率并保持一致性。

从管理事物到管理管理事物的代码，这一过程并非一蹴而就。例如，技术人员和公司高层可能会有抵触思想，或遗留系统可能含有手动配置组件，导致难以实现自动化。最后，即便是最灵活的 IT 团队，转变也并非易事。习惯了交接和人工交互的人们，适应自助服务和自动配置的速度可能比较慢。不过对于刚刚起步的组织，建立一个专门的团队来开发和部署自动化和自助服务，形成标准化的流程，可能会大有裨益。随着时间推移，团队可以有条理地拓宽其方法的应用范围，逐渐改造更多的流程。

幸运的是，目前已经有一些急需的自动化技术（以云服务的形式）可用。其余的是可以通过工程、对建立自动化未来的审慎和持续的关注来实现的。



先行者经验

云的自动化释放了开发人员敏捷性和创新速度

早在 2015 年，Capital One（美国第一资本金融公司）就指出，所有的新应用程序都会在云上构建和运行，所有现有的应用程序也会迁移到云上。考虑到当时企业内部基础设施的规模，加之几乎很少有企业能够完全在云上运营，这一目标看起来似乎过于宏大。但这家金融服务机构达到了目标，成为第一家摒弃传统数据中心、全身心投入公共云的美国银行。[4] 这样做的好处多多，其中最重要的是增加了自动化和快速扩展的机会。早在 2015 年，Capital One（美国第一资本金融公司）就指出，所有的新应用程序都会在云上构建和运行，所有现有的应用程序也会迁移到云上。考虑到当时企业内部基础设施的规模，加之几乎很少有企业能够完全在云上运营，这一目标看起来似乎过于宏大。但这家金融服务机构达到了目标，成为第一家摒弃传统数据中心、全身心投入公共云的美国银行。4 这样做的好处多多，其中最重要的是增加了自动化和快速扩展的机会。

当Capital One将更多的数据和应用程序转移到云上时，技术团队成员知道，他们不想简单地复制现有系统和流程。他们希望充分利用云服务的各种可能性，建立更现代的技术栈。这包括采用微服务、自动化、实时数据和机器学习等领先技术趋势。

“计算和存储仅仅是云技术的冰山一角，” Capital One 技术部负责云计算和生产力工程的高级副总裁 Chris Nims 说道[5]，
“如果你只是简单地将应用程序堆到云上，将无法获得云的全部优势。”

Capital One目前越来越频繁地利用无服务器计算模型，结合提供应用程序的容器、必要的资源库以及其他依赖关系，确保开发人员无需担忧寻找计算资源的问题。团队还建立了一种规则引擎，并将其开源，帮助组织定义各种策略，结合自动化治理、安全、合规和效率，更好地管理云环境。

这些移动部件看起来似乎很复杂，但团队发现，这样可以延长正常运行时间。利用现代技术堆栈则意味着能够部署自动化监控工具。机器学习应用程序监控实时服务器数据和系统应用程序，确保其运行正常，并在大多数用户注意到问题之前提醒技术人员。

“这些环节缩小了，我们知道原来人工监控的方式无法实现规模化应用，” Capital One 金融服务部首席技术官 Arjun Dugal 说道，[6]“我们不得不利用先进的云原生监控工具和基于机器学习的异常检测，彻底改变应用程序生态系统的监控方法。我们的策略已见成效，尽管潜在故障点的数量急剧增加，但实际发生的事故却减少了。”

在自动化基础设施的支持下，Capital One在技术人才争夺战中更具吸引力。Nims 指出，大多数人去学校学习计算机工程学是因为他们喜欢解决难题的挑战。当他们毕业后，他们并不想把时间浪费在申请审批、监控服务器性能或维护过时数据库上。这些事务的自动化处理，可以让工程师有时间处理更具影响力的项目，因此 Capital One 在人才招聘方面有一定的优势。

“优秀的工程师们希望在现代基础设施上工作，” Nims说道，“他们想要站在技术前沿。 而这很大程度上就表现在让工程师把时间花费在最重要的事情上。”

提高开发人员的工作满意度，不仅仅是为了吸引人才，也与商业价值有关。Dugal表示，Capital One 雇佣了11000 名技术人员，其中 85% 是开发人员，因此，他们的敏捷性即便只是略微增长，也能为公司带来巨大利益。“这样是为了消除机械的重复性工作，从而让他们专注于最高价值的事务，”他说道，“开发人员敏捷性越高，客户效益越高，创新速度越快。”

UiPath为IT自动化的成功铺平道路

自2005年以来，UiPath一直是领先的机器人流程自动化（PRA）平台供应商，该公司信奉并宣扬自动化技术所能实现的宏伟战略愿景，帮助客户踏上自动化之旅。它建立了一种运营模式，确保自动化持续改进并为客户创造价值。[7] 据UiPath公司客户战略和解决方案高级副总裁Jay Snyder所述：“自动化由 IT 授权和管理，但通过业务驱动。这就是巧克力和花生酱的结合点。”

在帮助数百家组织实现了业务流程自动化后，目前逐渐将其专业知识转向 IT 业务。UiPath运营与合作伙伴高级副总裁 Eddie O’ Brien 表示，高级领导者更多地参与 IT，有助于组织在 IT 部门内实现自动化技术的规模化应用：“人们往往只是在自动化环境中随波逐流，并不理解未来的方向。与IT部门更密切的接触可以带来更多的数字化转型。”

Snyder表示，如果自动化在IT领域使用得当，团队不仅可以控制自动化平台，还能向内转化，实现IT流程自动化，如工单创建、许可管理或网络安全响应等。这一愿景甚至超越单个流程，通过具有重大影响的 IT 服务自动化（如 DevOps 和数据管理），实现零接触 IT。Snyder 的团队与 IT 部门合作，创建了自动化用例的工作手册，优先处理流量最高、价值最低的任务。团队成员还创建了 IT人物画像，如系统管理员，指导 RPA 平台像 IT 员工那样，完成不同业务流程或部门之间的一系列任务。这样做，组织的 IT 人员可以专注执行更高价值的任务，或设计进一步的自动化。“人们往往关注的是通过自动化减少员工数量，但我们发现真正的好处在于成倍地提高生产力。” Snyder说。

这样实现在IT部门持续增长的一个自动化循环：随着数字化辅助的人员越多，团队成员产生的自动化创意越多，机器人融入 IT 流程的程度越高。此外，平台上的人工智能/机器学习可以分析组织的自动化流程，并给出改进或扩展建议。O’ Brien认为，实现持续 IT 自动化的关键第一步是落实正确的战略。目标是创建端对端自动化，推动数字化和业务转型。 O’ Brien说：“当我们将全自动企业愿景付诸实施时，会对 IT 效率以及目前的管理方式产生重大影响”。

自动化帮助安森保险在动荡的保险业内保持领先地位

安森（Anthem）保险公司为全美约4000万人们提供医疗健康保险服务。其首要任务是确保客户能够享受护理服务。这就是为什么近年来，该公司将大部分核心基础设施自动化，让工程师将更多的时间放在业务更优先的项目上，从而重新调整IT部门的工作方向，为“业务至上”的使命服务。

“整个行业已经从产品管理向产品构建转变，”安森保险云卓越中心员工副总裁 Srinivas Yamujala 说道，“为了保持安森保险的竞争力，我们必须积极推动数字化，灵活应对问题。为响应公司的转型倡议，我们重点聚焦端对端自动化，以简化基础设施服务和共享平台的交付流程，加快交付速度，从而更快地构建和发布应用程序和产品。”

这次过程中，重点动作之一就是向云转型。Yamujala表示，安森保险过去依赖传统的基础设施交付，通过繁琐的人工流程获取和提供基础设施。如果新客户要求增加服务器容量，可能需要三至六个月才能获得并完全配置好硬件。但是现在，安森保险把大部分的业务流程都转到云

上；原来需要数个月才能完成的流程，现在只需要两小时就能轻松搞定。安森保险开发出了一个安全的编排和供应自动化平台，符合医疗保险领域的监管和安全政策要求，且已申请专利。应用程序开发团队利用这个平台，能够在几分钟内按需提供资源。

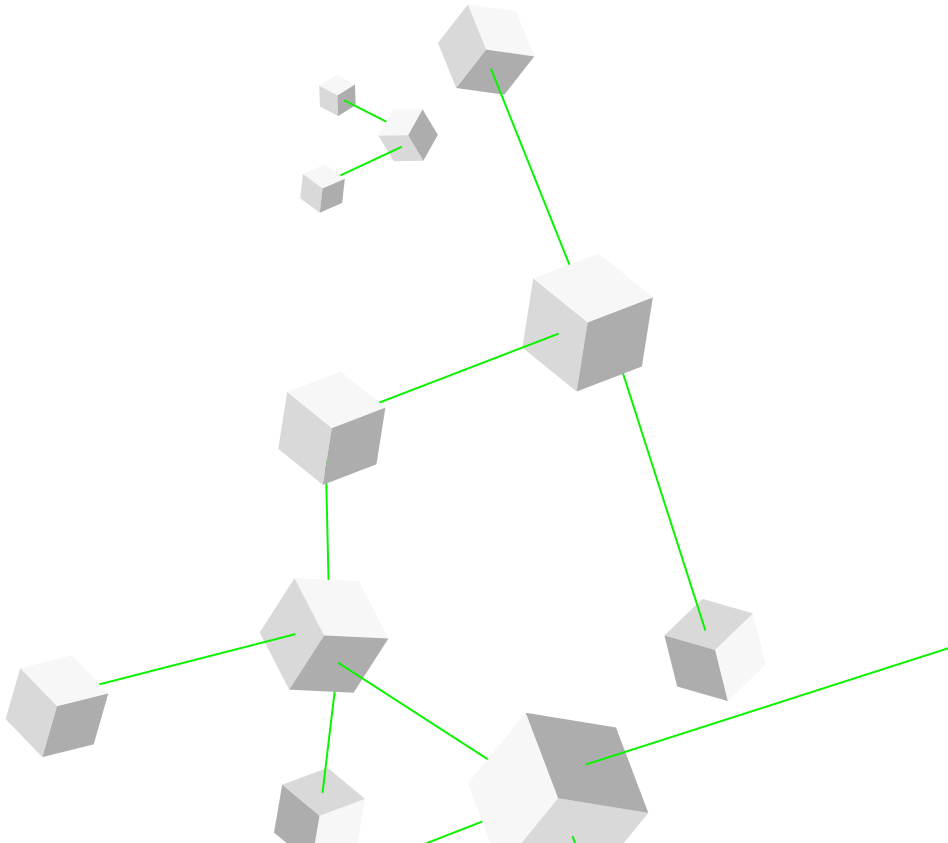
为了支持创新和转型，安森保险采用了云服务，并利用安森严格的安全协议“加固”了云服务，以及实现规范化处理。这些预先配置的服务被组合成一个服务目录，使应用程序开发人员能够利用满足法律和安全合规标准的若干原生云供应商服务。过去，开发团队要使用某种特定服务时，必须自行建立服务的防护措施，导致所用的方法各不相同，实施过程重复、繁琐。此外，处理应用程序时，开发人员过去必须向安全团队提交工单，申请打开特定的防火墙端口，这样其应用程序才能与其他系统和应用程序通信。现在，安森保险利用微服务和应用程序接口，将所有这些工作流程都转到自动化平台上。目前，开发人员管理复杂防火墙变更的需求已经尽可能减少，甚至，安森保险还利用零信任能力，努力消除这一需求。这极大地提高了开发人员的社区生产力，预计未来状况还会更好。

“我们希望助力我们的开发人员社区发展，”Yamujala说道，“我们的大部分自动化工作都是为了简化应用程序开发和部署流程。目前所见的大部分自动化都与’ 基础设施即代码‘相关，但是我们要超越现状，思考哪些可以帮助开发人员更快地解决业务需求。”

完全自动化的另一个优势是：有助于延长系统正常运行时间。要维护企业内部基础设施，工程师就必须监控服务器及其托管的应用程序。Yamujala 说，由于应用程序与硬件配置之间存在相互依赖性，工程师很难提前预判问题。现在，云服务使这个问题变得简单，系统性能也有所提高。

通过基础设施、平台以及应用程序开发和部署的自动化，所获得的收益不仅仅局限于 IT 部门。Yamujala表示，目前的业务范围更广，所处的位置也更好，可以更快地满足不断变化的业务需求和客户预期。

“在满足不断变化的行业需求、客户需求，并在不断变化的条件下维持公司业务的过程中，我们变得更加灵活、敏捷和快速。”Yamujala说道。



我们的观点

Bill McDermott

ServiceNow总裁兼首席执行官

C.J. Desai

ServiceNow首席运营官

在ServiceNow公司，我们认为我们的平台是整个企业数字化转型的控制塔。

如今的数字化世界里，IT 架构就是业务架构。制定实现技术基础设施全面自动化的统一方法，从未变得如此重要。

这是因为在 ServiceNow，我们自身就是“零号客户”。我们上市的所有产品都会先在公司内部使用。这样可以帮助我们观察自动化的影响，了解数字化活动协调的好处。它还能帮助我们理解：在支持整个企业数字化转型愿景的现代化IT组织中，自动化需要怎样开展工作。

但我们的平台启动后，我们支持规范化的工作流程；我们最初的应用领域是IT服务管理。随着时间推移，客户开始利用平台实现其他用例，比如网络安全运营、人力资源入职和离职管理、客户服务等。我们的平台目前已经发展成为能够支持基于机器学习的自动化，不久之后，还能为缺乏简洁接口的系统提供RPA能力。

但是，在任何数字化转型工作中，将离散的前端进程自动化都不是最终目标，真正的目标是理清混乱的中后端系统，并整合前端的自动化孤岛。多年以来，企业已经投入数十亿美元，确保其数字化前端和客户体验效果达到最好。然而，他们在后端系统和配套技术方面的投入就少得多，导致这些地方还充斥着许多手动流程。这拖慢了运营速度，把前端客户体验的优势降到了最低。

客户是不会接受这种情况的——他们希望，只要需要时，就能立即得到。他们希望拥有可见性。你的订货系统可能很好，但如果客户无法跟踪订单状态，那么整体客户体验也不会很好。

这就是为什么我们提倡摒弃过时的交易记录型系统，采用更现代的“行动系统”法。需要在整个销售过程中对接客户，而不仅仅局限于前端。这不需要投入更多人力。自动化就可以做到。

自动化不仅是为了满足客户预期。它还能有效提升员工体验。没有员工希望每天一成不变地做相同的任务。对于开发人员和工程师来说尤为如此；他们宁愿花时间解决高价值的复杂难题，也不愿做基础性的系统监控工作。同样地，各行业的企业也在竭力寻找所需的人才。人才战已经打响，而大多数企业都很难跟上步伐。低价值任务的自动化，可以让员工腾出手来，处理更高价值的问题。这就是提升员工体验，留住人才的最佳方法之一。

最终，这一切都会加速价值的实现。不论你的目标是联系客户，还是助力员工开展更高价值的任务，协调一致的自动化方法可以帮助你的企业以更快的速度实现收益。一旦实现作业自动化，实现价值的时间将缩减到数周到数月，而不再是数月到数年。

高管视角

战略

自动化技术应用于IT，有望提高效率、弹性和可扩展性。首席执行官应与 IT 领导密切合作，了解满足运营和战略目标的各种计划。这一举措可以帮助 IT 人员专注处理更多增值工作，所以领导者可以与首席信息官和其他技术领导者合作，重新关注和培训 IT 人员。这样可以激发个人成长和学习的热情，而不会对 IT 变化的忧心忡忡，同时还能探索技术在组织中的新作用，创造新的可能性。

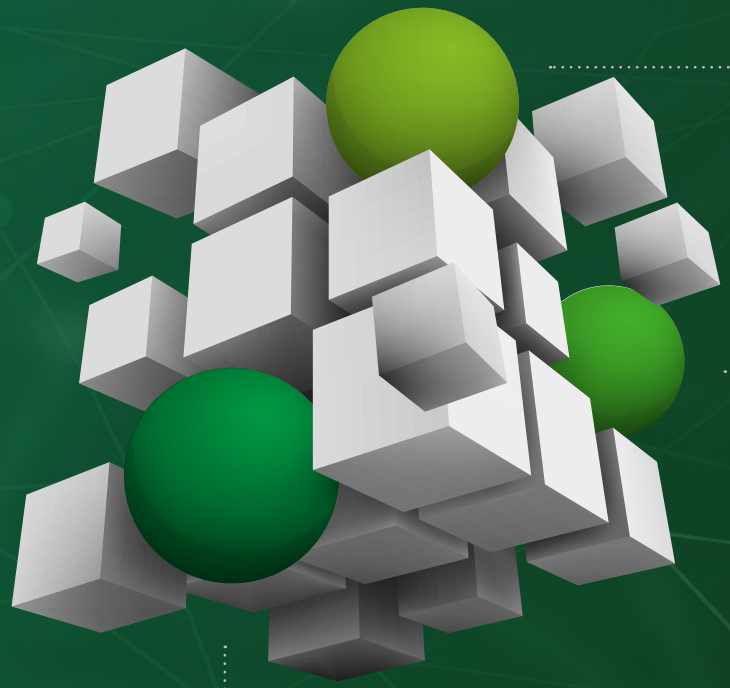
金融

随着科技人才的需求达到历史新高水平，首席财务官应欢迎向自动化的加速转变。从自动化处理单调的 IT 活动开始，自动化转型需要人才和资源两方面的前期投入。随着 IT 人才从日常工作中解放出来，企业可以以更高的弹性和更低的成本实现越来越复杂的自动化应用。而这还需要提高技能和更换装备，不过自动化转型为寻找不同的IT人才提供更多选择。

风险

随着公司 IT 自动化的程度越来越高，不良分子可能会寻找更多的攻击载体。在传统环境中，管理员接受过训练，会在停机和事故后恢复系统上线。若没有适当规划，自动化环境可能会带来一些挑战。当IT流程被数字化和自动化时，首席风险官应着重强调弹性。在其自动化进程中，组织可以从一开始就建立自己的风险管理原则，利用人工智能，更积极主动地应对突发威胁。

你准备好了吗?



关键问题

1 目前你的哪些基础设施和管理功能需要人工干预? 其中哪些可以实现标准化和自动化处理?

2 你的员工所从事的活动中, 价值最低的是什么? 它能被自动化处理或消除吗?

3 你的哪些自动化功能可以进一步优化? 你如何超越基于规则的决策, 探索优化机器学习?

了解更多

NoOps in a serverless world
继续阅读, 了解云计算的超自动化技术如何创建 NoOps 环境, 促进发挥业务成效。

Enterprise IT: Thriving in disruptive times with cloud and as-a-service
阅读 2021 年版的《一切皆服务 (XaaS) 研究》, 了解技术应用者如何从 XaaS 模型中获益。

Digital transformation collection
探索驱动效率、助力新产品服务、实现新商业模式的最新洞察

作者

我们的洞察可以帮助你把握新兴趋势的机遇。如果你在寻找应对挑战的灵感，那我们可以谈一谈。

Kacy Clarke

云架构市场化负责人
德勤管理咨询
kaclarke@deloitte.com

Ken Corless

云工程化业务总监
德勤管理咨询
kcorless@deloitte.com

Glen Rodrigues

代工服务市场负责人
德勤管理咨询
grodrigues@deloitte.com

Lars Cromley

云工程技术研究员
德勤管理咨询
lcromley@deloitte.com

资深撰稿人

Julien Kopp
合伙人，
Deloitte France

Andreas Zachariou
总监
Deloitte MCS Limited

Alice Doyne
高级经理
Deloitte MCS Limited

Kelly McLaurin
高级经理，
Deloitte Consulting LLP

Naoki Morinaga
高级经理，Deloitte Tohmatsu Consulting LLC

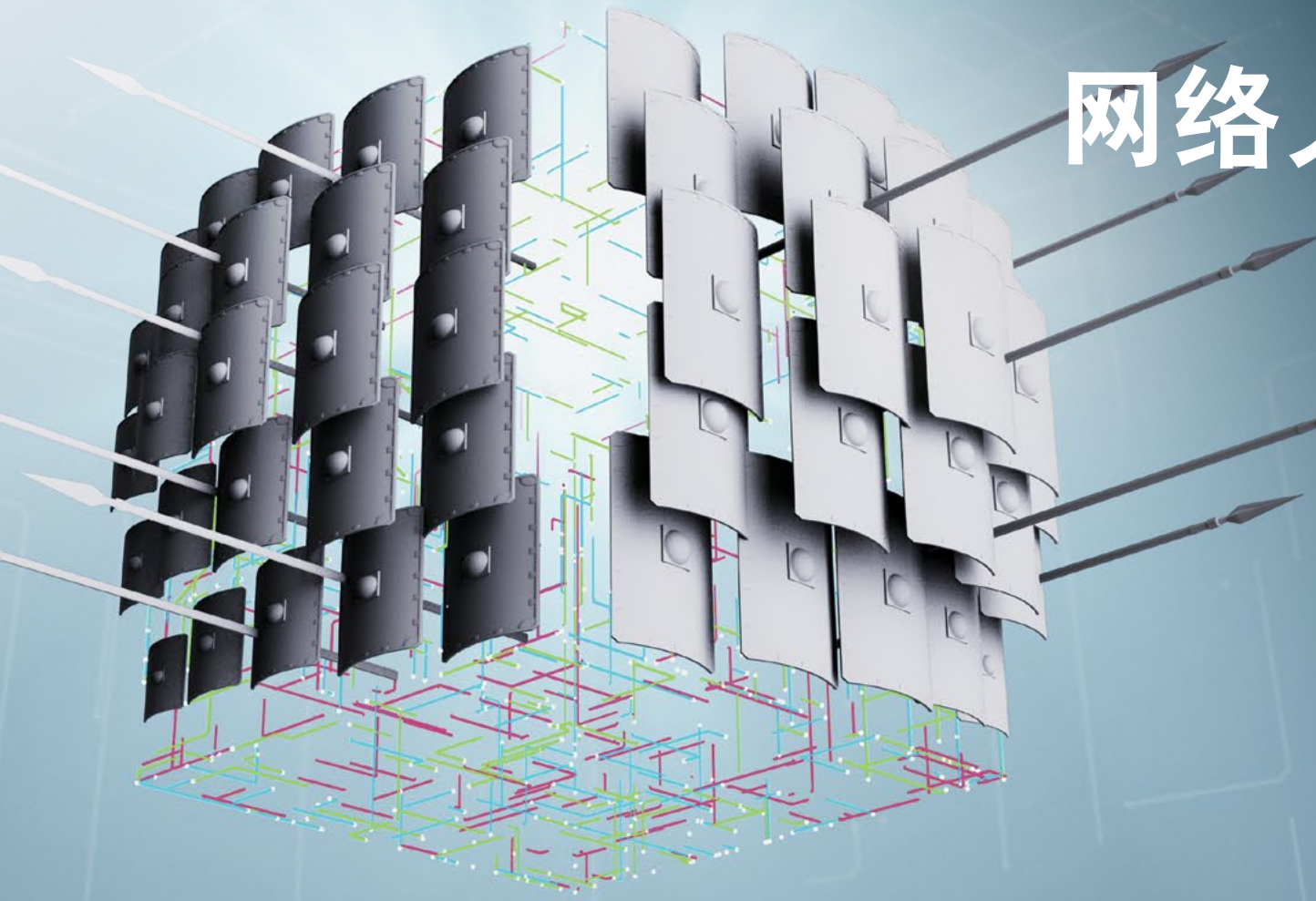
João Sanches
高级经理，Deloitte & Associados SROC, S.A.

Takashi Torii
高级经理，Deloitte Tohmatsu Consulting LLC

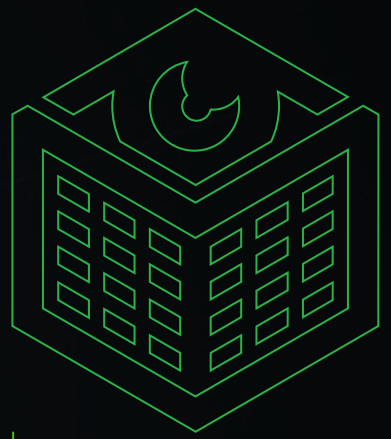
Bertrand Polus
经理，Deloitte Tohmatsu Consulting LLC

尾注

1. Salesforce, *IT leaders fueling productivity with process automation*, accessed November 9, 2021.
2. Ibid.
3. David Linthicum et al., *The future of cloud-enabled work infrastructure: Making virtual business infrastructure work*, Deloitte Insights, September 23, 2020.
4. "How Capital One Moved Its Data Analytics to the Cloud," *Harvard Business Review*, February 23, 2021.
5. Chris Nims (senior vice president for cloud and productivity engineering in the technology division, Capital One), interview, October 25, 2021.
6. Arjun Dugal (CTO of the financial services division, Capital One), interview, October 25, 2021.
7. Jay Snyder (SVP customer strategy and solutions, UiPath) and Eddie O'Brien (SVP operations and partners, UiPath), interview, October 27, 2021.
8. Interview with Srinivas Yamujala, staff vice president of cloud center of excellence, Anthem, Inc., November 5, 2021.



网络人工智能：有效防御



保护不断扩大的攻击面

随着越来越多的系统和数据上线，企业漏洞也越来越多。

缩小网络人才缺口

人工智能可以帮助企业解决网络安全人才长期不足的问题。

以牙还牙

人工智能安全工具可能是应对人工智能安全威胁的最佳防御手段。

趋势 5

网络人工智能: 有效防御

数据和机器智能增强安全团队的实力

虽然组织已经大力投资安全技术，但其仍然要继续应付各种破坏安全的行为：对手快速转变战术，始终保持技术领先。检测网络攻击涉及庞大数据、复杂性和高难度等问题，单靠人工可能很快就不堪重负。

人们目前不得不面临一项挑战，即高效分析从整个安全技术栈流入安全运营中心 (SOC) 的数据。这还不包括网络设备的信息反馈、应用数据以及更广泛技术堆栈的其他输入，而这些往往是高级攻击者寻找新载体或利用新恶意软件的目标。随着企业越来越多地向防火墙之外的区域拓展，安全分析师必须保护的攻击面也不断扩大。

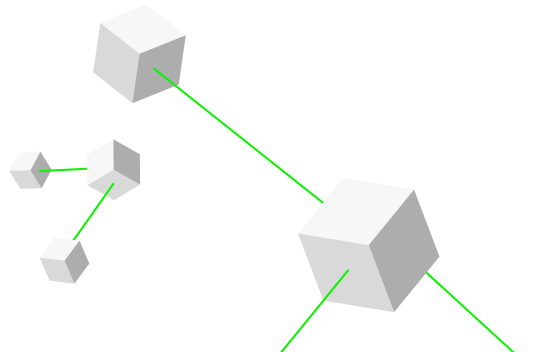
同时，网络犯罪导致的成本持续攀升。2015 年，网络犯罪成本为3万亿美元，预计到 2025 年上升至 10.5 万亿美元。[1]保险公司美国国际集团 (AIG) 指出，自2018年以来，仅赎金索赔一项成本就增长了150%。[2]

是时候向AI寻求支援了。网络人工智能可以成为一种力量的倍增器，使组织不仅能够比攻击者更快做出反应，而且能够预判攻击行为并提前作出反应。网络人工智能技术和工具正处于早期应用阶段，预计全球市场将在 2021 年到 2025 年间增长 190 亿美元。[3]

人工智能具备自适应学习和检测新模式的能力，能加快检测、控制和响应速度，减轻安全运营中心分析师的负担，提升分析师的主动性。人工智能的好处在于：可以帮助组织为应对人工智能驱动型终极网络犯罪形式做好准备。

不断扩大的企业攻击面

组织的攻击面正成倍扩展。正如我们在“技术堆栈实体化延伸”一章中所讨论的，应用 5G 网络、网络连接数量增加、员工更加分散、伙伴生态系统更加广泛等因素都可能引入新的风险。这些因素使企业不再受防火墙保护，将企业推进客户设备、员工家庭和合作伙伴网络中。



远程办公人员增多。在新冠肺炎疫情之前，居家办公人员的比例仅约为 6%。而到 2020年5月，约35%的受访者居家办公。[4]在2020 年刚开始封锁的前六周，针对居家办公人员的攻击占比从 12% 上升至 60%。[5] 调查发现，51% 的受访者开始远程办公后遇上了更多的钓鱼邮件。[6]

对于许多员工来说，预计远程办公仍将是固定办公方式而非例外情况，这为网络犯罪分子提供了许多新的机会。例如，由于处在企业防火墙和网络安全网关的安全保护范围之外，远程办公人员更容易成为攻击对象。远程办公人员依赖于家庭网络和 VPN 连接，并经常使用不安全的设备访问基于云的应用程序和数据。而传统的企业内部安全设备通常是为企业级网络而设计，而非基于家庭的互联网接入。

随着企业拓展到员工的家庭环境中，用户行为和数据活动更加多样化，且偏离常规。员工在异常时间从不常用的地点和设备登录会增加识别异常行为的挑战性，还可能导致误报情况增加。

联网设备增加。5G、物联网、Wi-Fi 6和其他网络方面的进步使得联网设备增加。越来越多的实体联网资产可能成为网络犯罪分子的软攻击途径。据估计，到 2023年，这类资产数量将达到 293 亿[7]。

连接到这些网络的设备数量达到前所未有之多，产生了大量需要处理和进行安全防护的数据，进而使安全运营中心发生数据堵塞。跟踪和管理活跃资产及其目的和预期行为是一项富有挑战的工作，由服务编排器负责管理活跃资产时，更是如此。

这类设备中的一大部分并非集中放置或受统一管控的，它们分布在各个远程地点，在多个边缘环境中运行和收集要返回企业的数据。缺少适当安全预防措施的情况下，设备可能会失陷，并在之后继续正常运行于网络中，实际上就会被入侵者控制，成为投放恶意代码或发起群体攻击的机器人程序。

跟踪和管理活跃资产及其目的和预期行为是一项富有挑战的工作，由服务编排器负责管理活跃资产时，更是如此。

第三方合作伙伴生态系统更广泛。长期以来，全球供应链和托管数据、基础设施和服务一直是导致第三方风险的因素，并且这类供应链以及托管数据、基础设施、服务的数量还在不断增加。随着越来越多的组织将数据与第三方应用集成在一起，API （应用程序接口）带来的安全问题日益显著。据 Gartner 预测，到 2022 年，API 滥用将成为企业受攻击最频繁的途径。[8]

第三方漏洞正变得日益复杂。五年前，入侵者可能会使用广泛可用的恶意软件来针对特定计算机系统，获得承包商凭证，窃取客户数据。这种情况虽然复杂，但那时我们尚能明确来源，也有能力监控和对破坏进行补救。

与利用复杂供应网络中安全性最低的嵌入组件实现相同目的的攻击相比，这类攻击相形见绌。一个没有边界的漏洞几乎无法监控和补救，活跃的窃取活动也可能持续多年。

5G 网络的应用。预计 5G 将通过新的连接方式、能力和服务完全改变企业网络。但是，企业向包括硬件和分布式软件定义网络、开放架构、虚拟化基础设施内的 5G 组合转变，将导致新的漏洞，扩大攻击面，需要提供更具动态的网络保护。

每平方公里 4G 网络仅可支持 10 万个联网设备[9]，而每平方公里 5G 网络则可支持多达 100 万个联网设备，创建高度可扩展和连接密集的设备环境。市场观察人士预计，到 2025 年，5G 移动连接数将达到 18 亿（不包括物联网），比 2021 年的 5 亿连接数更多；[10] 蜂窝物联网连接数量将达到约 37 亿，比 2020 年的 170 万连接数更多。[11]

随着公共5G 网络的扩大，政府、汽车、制造、矿业、能源等行业的组织也开始投资能满足企业低时延、数据隐私和安全无线连接要求的 5G 专网。自动驾驶汽车、无人机、智能工厂设备、手机等连接 5G 公共和专网的设备，应用程序和服务组成的生态系统为黑客提供了更多潜在入口点。因此，每项资产都需要通过配置来满足特定安全要求。而且，随着设备种类的增加，网络变得更加异质化，这给监控和保护带来了日益严峻的挑战。

人工智能防御当今网络威胁

网络安全人才的长期紧缺问题进一步加剧了攻击面不断扩大和网络威胁日益严重复杂的情况。据估计，全球网络安全专业人员缺口超过300万，相关领域的就业人数还需要增长约 89% 才能消除这一人才缺口。[12] 人工智能有助于填补这一缺口。

威胁检测加速。威胁检测是最早的网络人工智能应用之一，能够增强现有攻击面管理技术，降低噪音，让稀缺的安全专业人员集中精力处理最突出的入侵信号和指标。威胁检测还能更快速地做出决策并采取行动，关注更具战略意义的活动。

先进的分析和机器学习平台可以快速筛选安全工具产生的大量数据，识别偏离常规的数据，评估数千个遍布网络的联网新资产产生的数据，并通过训练区分合法或恶意的文件、连接、设备和用户。

人工智能驱动的网络和资产映射与可视化平台可就不断扩大的企业攻击面提供实时解读，识别和分类活跃资产，包括集装箱化的资产，从而使违规资产行为可视化。运用人工智能和机器学习的供应链风险管理软件可检测物理和数字供应链环境的过程自动化，并跟踪资产的组成和连接方式。

扩大控制与响应的利器。人工智能还可以作为一种力量倍增器，帮助安全团队将耗时的活动自动化，提高控制与响应效率。可以考虑机器学习、深度学习、自然语言处理、强化学习、知识表示等人工智能方法。结合了自动评估和决策的人工智能可帮助分析师管理日益复杂的安全威胁，并实现规模化。

例如，与前几代移动通信技术一样，5G容易受到干扰攻击，即攻击者故意干扰信号传输。来自弗吉尼亚理工大学英联邦网络计划的研究人员，正和德勤研究人员协作研究 5G 网络安全设计和实现，致力于在低级别的信号干扰导致网络瘫痪之前实别它。研究人员通过采用基于人工智能的干扰方案和机器学习模型，开发出一套实时脆弱性评估系统，可以检测出低级信号干扰，并对干扰模式进行分类。[13]

自动化有助于最大限度地发挥人工智能的影响，缩短从检测到修复之间的时间。嵌入人工智能和机器学习的SOC（安全运营中心）自动化平台可以采取自主的预防性行动，例如，阻止访问某些数据等的访问，并将问题上报到安全运营中心进行进一步评估。经用户访问模式训练的机器学习模型置于控制API 访问的 API 管理解决方案之上后，可检查全部 API 流量，实时发现、报告和处理异常情况。

积极主动的安全态势。经过适当训练的人工智能可以实现更积极的安全态势，提升网络韧性，使组织能够在受到攻击的情况下继续运作，缩短攻击者停留在组织环境中的时间。

例如，有丰富上下文的用户行为分析可以与无监督机器学习算法相结合，自动检查用户活动，识别网络活动或数据访问中的典型模式，识别、评估和标记异常（并忽略误报），决定是否需要响应或干预。人工智能通过向人类安全专家提供情报，使人类安全专家能够积极寻找攻击者，从而实现积极主动的威胁捕获。

组织可以利用人工智能和机器学习来实现安全策略配置、合规性监测、威胁及漏洞检测与响应等领域的自动化。例如，机器学习驱动的特权访问管理平台可以自动建立和维护安全策略，有助于执行零信任安全模式。通过分析网络流量模式，这类模型能够区分合法连接和恶意连接，并就如何分割网络以保护应用程序和工作负载提出建议。

通过将漏洞分析与强化学习相结合，安全专家可以生成攻击图谱，对复杂网络的结构进行建模，揭示最佳攻击路径，从而更好地理解网络漏洞，减少进行测试所需的人员数量。同样地，网络攻击模拟工具能够持续模拟高级威胁的战术和程序，从而突出基础设施的脆弱性和潜在攻击路径。

提升人类安全分析师的作用。在一项针对安全分析师的调查中，40% 的受访者表示他们最大的痛点在于警报太多；47% 的受访者表示他们难以知道哪些警报应该优先响应。[14] 另一项调查发现，分析师越来越认为他们的作用在于减少警报调查时间和警报的数量，而不是分析安全威胁和对其实施补救。超过四分之三的受访者指出分析师离职率超过 10%，近一半的受访者称离职率在 10% 到 25% 之间。[15]

人工智能无法取代人类安全专业人员，但可以促进他们的工作，并可能带来更高的工作满意度。在普通安全运营中心中，人工智能和自动化可以消除一级和二级分析师的繁琐工作。（一级分析师评估传入的数据并决定是否上报问题，二级分析师负责响应故障工单，评估每个威胁的影响范围，确定响应和补救措施，并在必要时上报。）这些分析师可以通过培训承担更具挑战性的战略性工作，例如成为高级二级分析师和三级分析师，去处理最棘手的安全挑战，并专注于主动识别和监测威胁及漏洞。

应对未来人工智能驱动型网络犯罪的利器

快速数据分析、事件处理、异常检测、持续学习和预测性情报这些特征既能使人工智能成为抵御安全威胁的有力武器，也会被犯罪分子用来发展新的或更有效的攻击和发现系统弱点。

例如，研究人员利用生成式对抗网络（即两个相互竞争以创建类似训练数据的数据集的神经网络）成功破解了数百万个密码。[16] 同样，GPT-3 开源深度学习语言模型也可以学习行为和语言方面的细微差别。网络犯罪分子可以利用该模型来冒充受信任的用户，使得人们几乎无法区分真实和欺诈性的电子邮件和其他通信。[17] 网络钓鱼攻击可能变得更加情境化且更可信。[18]

高级的攻击者已经可以渗透到网络并保持长期存在而不被发现，其行动往往是缓慢而谨慎的，有特定的目标。再加上人工智能恶意软件，入侵者可以学会如何快速伪装自己，逃避检测，同时攻击许多用户，迅速识别有价值的数据集。[19]

同样，GPT-3 开源深度学习语言模型也可以学习行为和语言方面的细微差别。

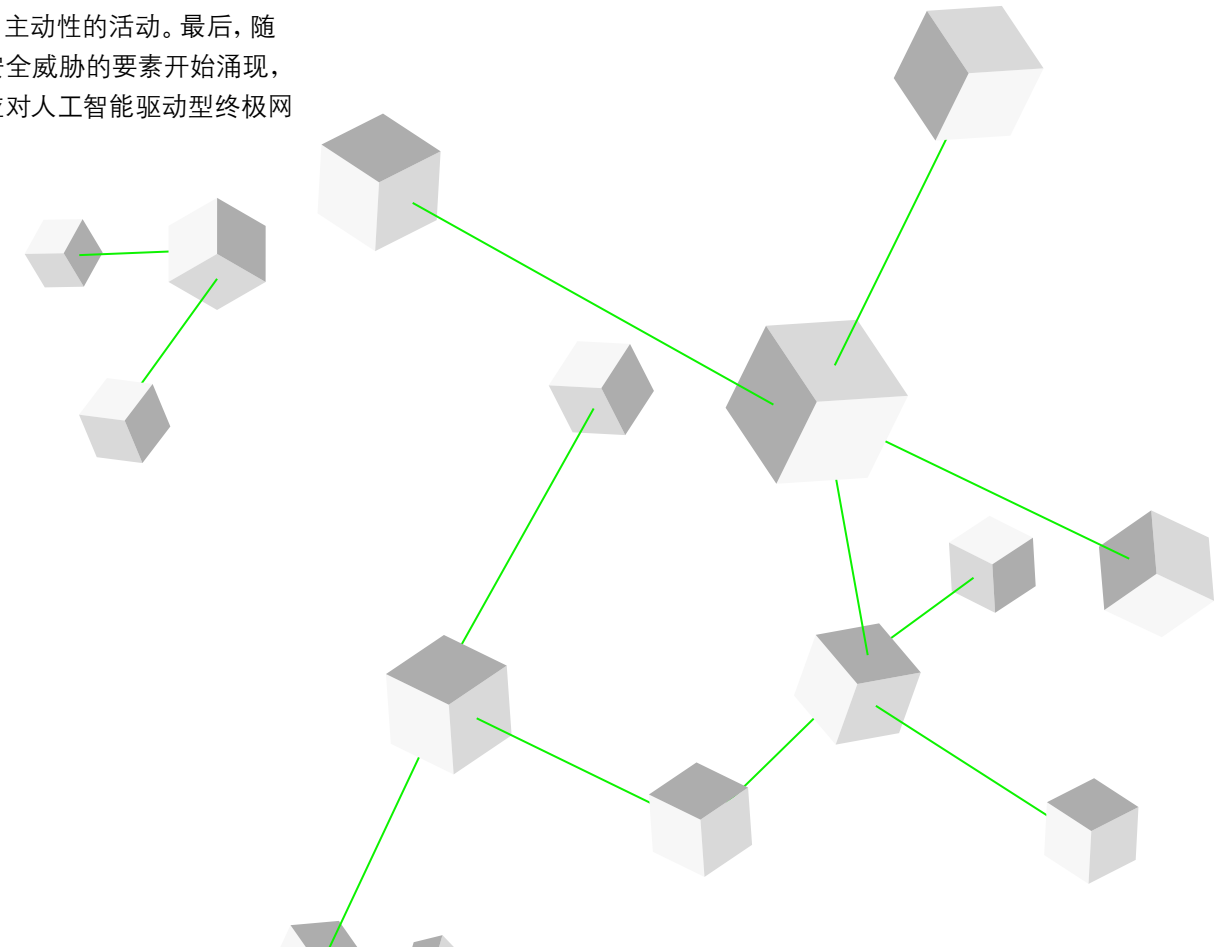
组织可以通过“以牙还牙”的方式来防止此类入侵：只要有足够的数据，人工智能驱动型安全工具就可以实时有效地预测和应对人工智能驱动型威胁。例如，安全专业人员可以将研究人员用来破解密码的技术用于测量密码强度或生成诱饵密码，帮助检测漏洞。[20] 上下文机器学习可以用来理解电子邮件用户的行为、关系和时间模式，以动态检测异常或有风险的用户行为。[21]

未来的方向

虽然许多组织才刚刚开始应用网络人工智能，但人类和人工智能在发现和防止漏洞方面的协作已经有一段时间了。然而，随着传统企业网络外的攻击面和暴露持续增加，人工智能能在更多领域发挥作用。

机器学习、自然语言处理和神经网络等方法可以帮助安全分析师区分信号和噪声。人工智能可以通过模式识别、有监督和无监督机器学习算法、预测性分析和行为分析助力识别和抵御攻击，自动检测异常用户行为、异常网络资源分配或其他异常情况。人工智能可用于同时保障企业内部架构和企业云服务的安全，尽管相比于企业内部环境来说，企业云中的工作负载和资源安全保障工作的难度往往较小。

就其本身而言，人工智能（或任何其他技术）本身无法解决当下或未来复杂的安全挑战。人工智能识别模式的能力和在事件发生时自适应学习的能力可以加快检测、控制和响应的速度，有助于减轻SOC分析师的沉重负担，并使分析师更加主动。对分析师的需求也许会继续保持旺盛态势，但人工智能将会改变分析师的角色。组织可能会要求分析师学习新技能或进行再培训，以帮助分析师从警报分类等低级技能转向更具战略性、主动性的活动。最后，随着人工智能和机器学习驱动型安全威胁的要素开始涌现，人工智能可以帮助安全团队为应对人工智能驱动型终极网络犯罪做好准备。



先行者经验

Sapper Labs 以软件对抗软件

为帮助加拿大和美国的军队、政府和关键基础设施运营商应对安全挑战，Sapper Labs (Sapper Labs Cyber Solutions) 提供网络安全思想领导、情报、研发、实施、运营安全平台和培训支持，来解决复杂问题。人工智能是 Sapper Labs 技术工具箱中日益重要的一个工具。

Sapper Labs 是一家网络防御公司，总部位于渥太华。该公司名称取自军事术语，即通过监视、侦察、防御工程及其他主动防御活动支持地面部队的作战工程师。Sapper Labs 启动其项目的假设是，所有网络、系统和能力已失陷，组织完全没有人力来防御或回击。Sapper Labs 创始人兼首席执行官 Al Dillon 指出："人才管道的增长既没有跟上攻击面的增长，也没有跟上商业和政府创新议程的扩张，因此我们无法产生足够的人才来保护我们的机构和资产。而这就是人工智能可以提供帮助的地方。"[22]

为此，Sapper Labs 目前正与多个加拿大和美国安全、国防与情报组织合作，创建人工智能系统，旨在实时灵活应对攻击者不断演变的威胁战术和程序。这些系统能做的远不止是提供决策依据，还可以学习如何在人类参与或不参与的情况下防御威胁。Dillon 表示："如今，利用机器学习、人工智能和自动化的网络防御主要集中在人类主导的网络参与方面。鉴于如今创新步伐以及网络和设备数量激增的速度如此之快，在组织之外更是如此，我们需要嵌入式自动化系统能力。"

Dillon 表示，国家安全和国防组织，以及其他公共和私营部门组织的集体目标应该转向军事级别、软件主导的参与：人工智能驱动型软件对抗人工智能驱动型攻击。他解释道："我们都面临着受国家行为者和其他具有同等意图、专业知识和工具的不良行为者的攻击威胁。"

例如，Sapper Labs 和政府机构正在开发一个多层威胁检测系统，该系统融合了各种来源的信息和数据，即所谓的全源情报 (all-source intelligence) ——涵盖从卫星、陆地和海源传感器、社交媒体等数字来源以及其他公网、专网信息。以传统方式可能需要安全团队花费几个月甚至几年的时间来检查这些数据。通过将这些数据和情报自动综合，并在此过程中应用算法，可使评估和决策速度比传统方法快 10 倍甚至 15 倍。Dillon 预计，未来三年，网络人工智能和自动化技术将快速发展，以至于能以比过去快 50 倍的速度评估情报、得出结论、做出决策。

Dillon 指出，这其中包含着网络人工智能最棘手的问题之一。他说道："克服网络人工智能所面临的人类、社会和文化挑战比解决技术问题要困难得多。需要跨越的最大障碍在于，即便人类领导者的决策过程比人工智能要慢 50 倍，人们也更愿意接受人类领导者所做决策，我们需要在此背景下让人们相信人工智能做出的决策。"

教育是建立这种信任的关键之一。目前，Sapper Labs 正在努力通过与其他私营企业、公共部门组织和学术机构展开合作，促进自动化网络安全意识在广泛范围内树立。Dillon 表示："我们正处于激动人心的技术应用和创新转型期，但令人震惊的是，我们尚未完全理解保卫国家安全、个人数据、知识产权和其他珍贵资产所能产生的社会影响。我们必须内化这样一种意识：使用人工智能的安全平台可能会成为我们始终领先于不良行为体的唯一途径。"

我的观点

Mike Chapple

圣母大学
信息安全负责人
兼IT、分析与运营授课教授

去年，网络安全攻击的性质发生了转变。

在此之前，勒索软件攻击是组织的主要关注点之一。勒索软件攻击是指不良分子通过钓鱼软件或互联网恶意软件获取企业数据，然后对数据进行加密以索取赎金。这种攻击是具有投机性质的，因为犯罪分子不能预测谁将“中了圈套”，且如果组织被攻击方有数据备份，那么它们就不一定能勒索成功。

如今，由于不良分子的犯罪性是有组织性的（类似于国家间的网络战），风险变得更高。我们已经看到新冠疫情期间医院成为目标，管道无法输送燃料，以及其他具有高度针对性的攻击。不良分子的新模式是对被盗企业数据提出两种勒索威胁，包括劫持数据和威胁泄露客户记录和知识产权等敏感信息。这类威胁对大型组织来说尤为突出，因为它们拥有网络犯罪分子想要的资金和数据。此外，由于 5G 移动网络的应用和居家办公政策等趋势将企业技术推向传统边界以外，这类犯罪的攻击面也在不断扩大。

组织如何应对这种风险加剧的氛围？组织有两种选择：雇佣更多人员，但这很困难呢，因为人才市场上相关技能缺口正快速扩大；或者依靠人工智能、自动化和分析来实时检测和应对威胁。近期的技术转变使得第二种选择（网络人工智能）变得日益有效。

人工智能和网络安全的交集已经被讨论了近十年。直到现在，这类讨论还是围绕着流行词和基于规则的产品展开。由于计算能力和存储能力的进步，我们现在看到，网络安全供应商开始在其产品中真正纳入机器学习和人工智能。如今，大型企业可以依靠这类供应商来推进威胁情报。

优秀网络安全供应商的产品遍布许多企业，这些产品是采集数据的传感器。通过将人工智能应用于每个客户的匿名数据中，供应商可以利用某个组织的威胁数据在其他组织中寻找类似的漏洞迹象。这可以产生指数级的网络效应：数据集越大、越多样化，供应商的检测效果就越好，其提供的保护就越强。因此，大中型企业都可以通过与托管服务提供商合作受益。或者，企业也可以让其内部数据科学和网络安全团队展开合作，在自己的网络安全仓库中训练人工智能模型。

如今的计算能力已经能够开发复杂的用户和实体行为分析（简称“UEBA”），检测不良分子或非常规行为的特征。UEBA可能会标记出一个被发现在周六上午下载TB级数据的用户——这种行为显然不同寻常。通过将这些用户画像和模式结合起来，就可以更精细地识别威胁。

尽管这些信号始终存在，但以前要分析这些信号并找出有意义的模式却是不切实际的。而现在，人工智能标记的威胁可以被送入安全协调、自动化及响应（SOAR）平台，这些平台可以关闭访问权限或立即采取任何其他行动。

网络安全的历史是一场由来已久的猫鼠游戏，实际上，任何类型的安全都是如此。正如我们开发人工智能工具来保护自己一样，攻击者也正在开发人工智能来进一步提高攻击的复杂性。各国已经进入了该领域，我们可能会在未来一年半到两年内看到更多来自私人网络的犯罪行为者。组织如果不想成为受害者，就需要立刻采取行动，寻找利用人工智能的机会，从而确保用户、系统和数据未来的安全。这样，当网络攻击的性质不可避免地再次发生转变时，组织就能做好准备。

我的观点

Adam Nucci

美国陆军
战略作战副主任

美国陆军正处于现代化进程中，需要采用数据驱动的思维方式，迎接数字化转型。

我们的目标不仅是发展武器系统和平台，还要发展过程、劳动力和文化。

随着我们的现代化发展，现在本来已经非常复杂的技术环境变得更加动态活跃，我们在各方面都面临着各种对手的挑战。为了实现我们宏伟的现代化目标，我们要做的最重要的一点就是提高安全态势。幸运地是，未来就在眼前：目前我们拥有现代化所需的工具。不过还需要集中精力，不仅要保证安全，还要转变提供能力、网络和人才的方式。建立自适应安全至关重要。目前各种技术系统和传感器正在不断生成大量数据。我们可以利用先进的分析技术和平台，快速分析和处理数据。云计算的广泛应用，实现了实时数据共享，以及全谱数据和网络管理、控制和可见性。

我们已经有各种积木式部件。数据、分析和云计算强力组合，构成了以数据（而非网络）为中心的零信任安全方法的基础，特别是从基于网络的身份和凭证管理，向以数据和设备中心的身份访问管理和最低权限访问原则迁移。这为网络人工智能的大规模应用奠定了基础。

利用机器学习、深度学习和其他人工智能技术，组织可以理解横跨多个硬件和软件平台之间的网络安全环境；确定数据储存的位置、数据的行为模式，以及与数据互动的对象；建立攻击者档案，并在整个网络环境中传播。人工智能和预测分析还可以帮助我们更好地理解网络安全中人为方面的因素。在整个运营环境乃至整个社会中，信息维度与万事万物存在着千丝万缕的关系；先进的机器学习和人工智能可以帮助我们理解信息领域影响用户的方式、我们的决策方法，以及对手的行为模式等。

目前的人工智能并不能普遍适用；大体上讲，它是一种有针对性的解决方案，少数情况下针对有限的领域，但绝大多数情况下针对特定的用例。但网络安全并非小问题，仅利用技术无法解决；它主要是关于人类的问题。我们的对手多种多样，极具创造力。是什么激发了他们？为了推进网络人工智能，在网络劳动力方面，我们也要保持同样的多样性和创造性。我们需要让以下两类人员进行思想交流：1）传统的接受过STEM教育，保持线性思维的网络人员，与2）特立独行的应用程序人才，以及可以根据模糊联系进行推理的多态思维人员。这样不仅能够在建模和训练中增加人类的维度，还可以创造网络安全力量倍增器。

在数据、分析和云的驱动下，基于人工智能的网络战略，可以助力组织自动预测、检测和反击入侵行为。移动和低带宽环境下还存在各种新的挑战和机会，不过我们已经打好了技术基础。

为了进一步实现网络人工智能，我们还需要强化公私部门之间的协调合作。网络安全就是 国家安全。社会需要将网络安全的地位，从事后补偿工具提升到所有商业和政府系统内嵌主干的位置。但是仅靠公共部门，这根本无法实现。通过建立稳定的公私合作关系，实现行业、学术界和国际合作伙伴之间的交流，我们可以基于传感器嵌入式系统、数据以及人工智能驱动的预测分析，构建稳固的网络安全基础。

高管视角

战略

网络风险是一个比以往更重要的战略问题。随着组织收集大量数据，以及企业的伙伴关系和员工群体变得更加广泛，保护工作也变得越来越复杂。网络人工智能已经成为防范近期大量复杂网络攻击的领先做法。首席执行官应该询问其首席风险官、首席信息安全官、首席信息官和其他人，了解当前的安全态势，以及是否需要进行升级。通过将人工智能定位为安全和战略优先事项，领导者可以来帮助组织认识加强防御和管理风险的重要性。

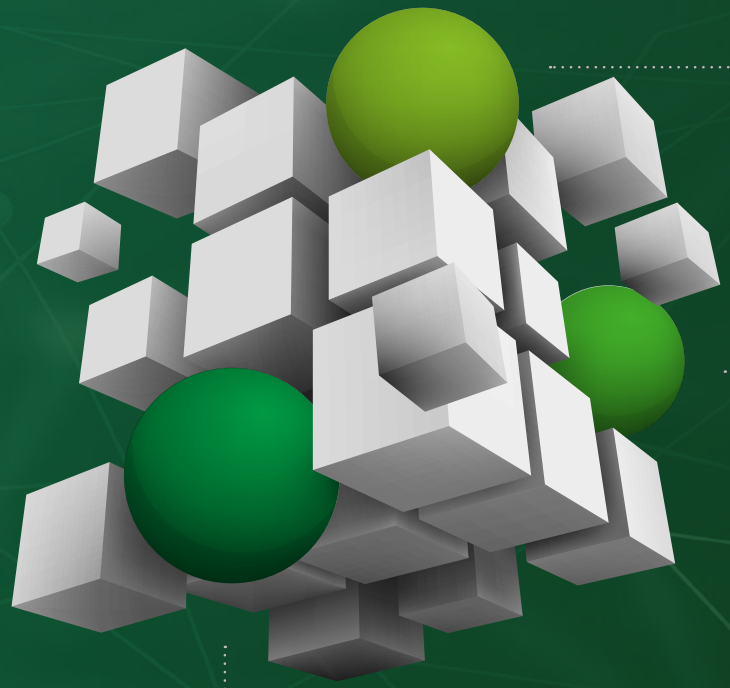
金融

随着网络攻击变得普遍和产生更大的财务影响，首席财务官在监督风险管理方面将发挥更大作用。作为公司最高管理层一员，他们应该发挥特有的职能作用，确保充分供资以支持采用人工智能技术增强网络安全防御，并倡导在公司范围内全面推行相应机制。他们可以与公司内部网络安全团队合作，了解网络人工智能方面所需的投资、时间安排、风险和好处，然后将这些信息作为关键优先事项提交给董事会。

风险

数年来，不良分子一直在利用人工智能进行网络攻击。通过人工智能安全防护手段和智能化安全操作来对抗这些攻击将成为新常态，各首席风险官应确保自己的组织为适应新常态而做好准备。组织应寻求内部支持来培养相应的新能力，或评估网络保护的外包，以增强其安全团队实力。当然，人工智能防御系统也存在自己的缺陷，而威胁格局将继续演变。现在就开始行动，逐步改进防御措施，而不是在为时已晚的情况下才做出反应，可以帮助组织保护客户及其数据。

你准备好了吗?



关键问题

1 远程工作者数量、网络连接设备数量以及第三方风险的增加，您的企业受攻击面是如何扩大的？您当下采取了哪些网络安全防护措施？

2 您目前如何使用人工智能工具来检测、遏制和应对网络威胁？在哪些领域可以扩大对人工智能的应用，从而创造更积极的安全态势？

3 实现当前的网络安全目标所需的技能组合及组织结构是否已经到位？如果还没有，两年之内能否做好准备？您计划如何掌握这些技能？

了解更多

Zero trust: Never trust, always verify
看看零信任网络安全态势如何为打造更稳健、更有弹性的安全机制提供机会。

2021 Future of cyber survey
从全球近 600 位对其组织网络安全职能有深入了解的高管那里获得洞察。

State of AI in the enterprise, 4th edition
探索当今由人工智能驱动的组织正在采取哪些不同方式引导自身走向成功。

作者

我们的洞察可以帮助你把握新兴趋势。如果你在寻找应对挑战的灵感，那我们可以谈一谈。

Curt Aubley

网络与策略风险工作组业务总监
Deloitte & Touche LLP
caubley@deloitte.com

Ed Bowen

人工智能 CoE 咨询负责人
Deloitte & Touche LLP
edbowen@deloitte.com

Wendy Frank

网络 5G 负责人
Deloitte & Touche LLP
wfrank@deloitte.com

Deb Golden

美国网络与策略风险负责人
Deloitte & Touche LLP
debgolden@deloitte.com

Mike Morris

网络与策略风险管理总监
Deloitte & Touche LLP
micmorris@deloitte.com

Kieran Norton

Cyber & Strategic Risk infrastructure security solution leader
Deloitte & Touche LLP
kinorton@deloitte.com

资深撰稿人

Wil Rockall
合伙人
德勤

Jan Vanhaecht
合伙人
Deloitte 比利时 CVBA

Sam Holmes
高级经理
德勤

Ryan Lindeman
高级经理
Deloitte & Touche LLP

PaPa Yin Minn
主导专家
Deloitte Tohmatsu Cyber LLC

尾注

1. Steve Morgan,"Cybercrime to cost the world $10.5 trillion annually by 2025," Cybersecurity Ventures, November 13, 2020.
2. IBM, *Cost of a data breach report 2021*, accessed November 17, 2021.
3. Ibid.
4. *CNBC*,"Cybercrime could cost $10.5 trillion dollars by 2025, according to Cybersecurity Ventures," March 9, 2021.
5. *PR Newswire*,"Artificial intelligence-based cybersecurity market grows by $19 billion during 2021-2025," June 21, 2021.
6. NCCI,"Remote work before, during, and after the pandemic: Quarterly economics briefing—Q4 2020," January 25, 2021.
7. Jasper Jolly,"Huge rise in hacking attacks on home workers during lockdown," *Guardian*, May 24, 2020.
8. Fleming Shi,"Surge in security concerns due to remote working during COVID-19 crisis," Barracuda, May 6, 2020.
9. Cisco, *Cisco annual internet report (2018–2023) white paper*, accessed November 17, 2021.
10. Gartner,"API security: What you need to do to protect your APIs," accessed November 17, 2021.
11. David Flower,"5G and the new age of fraud," *Forbes*, December 30, 2020.
12. GSMA, *The mobile economy*, accessed November 17, 2021.
13. Steve Rogerson,"Cellular IoT connections grew 12% in 2020, says Berg," IoT M2M Council, August 4, 2021.
14. (ISC)²,"(ISC)² study reveals the cybersecurity workforce has grown to 3.5 million professionals globally," accessed November 17, 2021.
15. Wendy Frank (Cyber 5G leader at Deloitte & Touche LLP), interview, October 1, 2021.
16. Palo Alto Networks, *The state of incident response 2017*, accessed November 17, 2021.
17. Critical Start, *The impact of security alert overload*, accessed November 17, 2021.
18. Matthew Hutson,"Artificial intelligence just made guessing your password a whole lot easier," *Science*, September 15, 2017.
19. Lily Hay Newman,"AI wrote better phishing emails than humans in a recent test," *Wired*, July 2021.
20. William Dixon and Nicole Eagan,"3 ways AI will change the nature of cyber attacks," World Economic Forum, June 19, 2019.
21. Ibid.
22. Matthew Hutson,"Artificial intelligence just made guessing your password a whole lot easier."
23. Tony Pepper,"Why contextual machine learning is the fix that zero-trust email security needs," Help Net Security, February 16, 2021.
24. Al Dillon (cofounder and CEO, Sapper Labs Cyber Solutions), phone interview with authors, October 19, 2021.

技术堆栈实体化延伸

实现系统

处理关键任务的物理系统绝不能发生故障。

重新考虑管控

智能设备带来了新的管控难题。

革新技术专长

需应用新的、不同的IT技能组合，来管理、监控和维护智能设备。

趋势 6

技术堆栈实体化延伸

首席信息官愈发需要对实体技术堆栈加以管理

随着先进的处理器和传感器、工业机器人和机器学习技术得以广泛应用，任何设备都可以被智能化、相互连接，还能够捕获数据并建立反馈回路，从而改进产品和服务，并产生新的收益流。随着实体设备种类呈爆炸式增长，且功能范围急剧扩大，首席信息官 (CIO) 的职权范围正再次扩张，超越了数字领域，全面覆盖这些新的实体资产。

几十年来，IT 组织的工作重心一直放在管理技术、工具、应用程序、框架、数据生态系统以及其他主要是数字技术堆栈的要素。过去，实体技术堆栈的动态程度要低得多，主要由员工接入点和数据中心基础设施组成。

随着技术越来越多地被运用于开展实际生产和运营工作，它正在从业务使能因素发展变化为价值驱动因素，成为做好企业的关键。如今，企业上下要做好智能设备管理工作，应当具备安全保障、自动化、数据驱动分析和决策、人工智能 (AI) 和机器学习等方面的数字化能力。例如，想想看，到 2025 年，新工业控制系统中有 30% 将具备分析和人工智能边缘推理功能，而 2021 年这一比例还不到 5%；[1]或者，预计到 2025 年，联网乘用车每月将产生 10 EB 的数据。[2]

从制造厂里用的铣床、基础设施中的联网心脏监测器，到餐厅使用的机器人炊具、办公楼内的智能传感器，乃至新的“数字实体”消费产品，新一代实体资产正被嵌入先进的数字技术，以实现多种业务关键功能。IT 组织要承担起管理、监控、衡量和保护这些资产的责任，这种需求越来越迫切。首席信息官必须根据应用、设备和安全性要求明智地选用技术，并考虑将如何搭载、管理并维护当前需要最大化正常运行时间和最高冗余度的设备及网络技术。他们还必须重新思考如何开展设备管控和监督工作，并重新考虑如何组织、定义、管理和培训技术队伍。

针对正常运行时间、冗余度和安全性增加竞争筹码

属于新实体技术堆栈的设备中，有许多都提供面向客户的业务关键型应用程序和服务。它们往往会生成和使用大量数据和视频，需要快速传输并分析这些数据和视频，以促进实时制定关键决策。

与前几代实体设备不同的是，如今的实体设备故障停机也许并不仅仅是带来不便——可能会威胁到业务运营（如果某家餐厅的点餐系统瘫痪，饥肠辘辘的食客便会去别的地方就餐）甚至危及生命（如果植入式心脏监测设备脱机，可能导致关键的患者数据被忽略）。

保持弹性至关重要。可能需要实现系统的正常运行时间最大化，并达到最高水平的可靠性和安全性。 随着实体技术堆栈对业务运营的影响不断扩大，组织可能需要考虑如何管理和维护新一代联网设备、无线网络以及边缘计算应用，从而按最高标准确保业务连续性。下文列出了部分最重要的领域。

设备和数据管理

为了优化设备和系统性能，IT 组织可能需要（通常以远程方式）部署和管理由多家供应商提供的联网设备、应用程序及网络构成的生态系统。可能需要采用新的平台、工具和方法来监控设备运行状况，检测和解决问题，并管理软件和固件更新。团队可能需要在设备中构建多层冗余。

要想将重复的、手动的设备管理任务从日程中剔除，实现自动化是关键，对于大型部署尤其如此。自动化设备管理工具可以帮助组织实现设备注册、配置、供应、维护、远程和空中固件及软件升级以及监控活动规模化。

为了提高性能或开发新产品和服务，组织可能需要对这些设备产生的大量数据加以管理。数据采集频率、处理时间、准确度和格式等问题都需要纳入 IT 部门考虑范围。数据存储将是至关重要的，而对于远程环境而言，分布式存储和边缘计算可能更为可取。

无线网络连接

为确定将这些设备连接到网络时应采用的最有效且最具弹性的解决方案，IT 部门需要对多种属性进行评估，如功耗、信号强度和范围、与实物和结构或天气和环境因素相关的干扰、电气或射频干扰、成本、连接中设备的数量、频率共用、安全性、弹性以及对持续稳定互联网连接的需求等等。

许多智能设备在客户所在地或其他远程、现实环境中运行，并通过先进的无线连接技术（包括 5G、Wi-Fi 6、低功耗蓝牙、多跳网络和卫星）加以启用。此类技术实现了高吞吐量、低延迟和大容量，从而使更高数据速率成为可能。

德勤在 2020 年进行的一项调查显示，受新冠疫情影响，企业加速了对更新的无线网络技术，尤其是 5G 和 Wi-Fi 6 的投资步伐。调查的参与者认为，5G 和 Wi-Fi 6 对于业务计划而言是最关键的两种无线技术。[3] 与之前的技术相比，这两种技术在性能和操作方面都有很大的改进，有望大规模支持设备、用户和流量，实现沉浸式体验，并帮助组织提升弹性。这两种技术都能支持基于物联网 (IoT) 及其他利用低延迟特性在边缘收集和共享大量实时数据的新兴技术的新应用。

无线网络技术是相辅相成的，数项技术可以同时存在或组合使用以支持多种用例。为保证即使遭遇毁灭性风暴也能持续运行，许多组织采用了不同能源技术并实现能源供应来源多样化。而各组织可能也需要采取类似策略，实现无线网络技术运用的多样化，以确保冗余。

边缘计算

尽管 5G 和 Wi-Fi 6 在性能上得到升级，但诸如自动驾驶汽车、智能工厂、增强现实和虚拟现实等应用要求网络延迟低至数十毫秒甚至降至亚毫秒级，而云计算无法确保对于此类应用可接受的响应时间和数据传输速率。当需要实时处理设备生成的分散数据时，采用边缘计算等分布式计算解决方案进行处理，比使用公共云或数据中心更为高效。

由于计算能力更接近数据源，边缘计算架构提供了实时管理、处理以及从海量数据中提取价值所需的延迟和带宽。但我们不能称之为再度盛行，因为边缘计算已存在数年。最近的一项调查显示，72% 的 IT 领导者已经在使用边缘计算技术；[4] 据 Gartner 预测，到 2025 年，企业所管理的数据中有 50% 以上将在数据中心或云之外创建并进行处理。[5] 增长蓄势待发：一家边缘计算行业组织预计，2019 年至 2028 年期间，在边缘计算装置和设备方面的累计支出将达到 8000 亿美元，其中，制造业和医疗保健领域发生的增长最为显著。[6]

72% 的 IT 领导者已经在使用边缘计算。

考虑到边缘计算站点的业务关键性质（通常情况下无人值守），冗余电源、冷却和网络连通性至关重要，同样重要的还有实体安全以及远程监控和管理。

管控和监督新路向

管控和监督策略及政策可能需要演化发展，以满足新一代联网设备的需求。对于 IT 组织来说，与实体设备和网络使用相关的法规及标准可能是陌生且具有挑战性的，并且多年来一直在不断变化。想想看，美国法院花了将近 20 年的时间，方针对电商销售税作出最终裁决，取代了缺乏统一性的各州税收法规。

下文给出了管控方面的一些关键考虑因素，涉及设备、数据和安全。

设备

经营某些实体资产可能受到美国联邦、州或地方限制令的约束。例如，使用户外无人机的美国组织必须就其进行注册并获得美国联邦航空局的空域授权；某些类型的无人机必须携带机载无线识别系统。[7]

同样，各国甚至美国各州针对自动驾驶汽车应用出台的监管法律也不尽相同。美国并不存在相应的联邦条例，只有各州自行制定的五花八门的法律来管控商用车辆的使用、驾驶员执照、驾驶员行车规范、速度限制和责任保险等事宜。[8]

责任的界定可能会变得越来越复杂。例如，如果某台由计算机驱动的智能设备出错，造成了人身伤害或财产损失，应由谁来负责，是供应商还是操作者？如果由人工智能驱动的决策造成伤害，将带来怎样的后果？可能会建议或要求为某些设备投保。

另一个问题是远程管理设备的所有权和维护，包括安全保障、保养和维修工作的责任划分，以及这对服务水平的影响。应将资产退役纳入设备生命周期管理工作，并制定替换单项或多项资产、注销证书、归档数据和删除机密信息的相应计划。

设备采购可能会带来新的挑战，比如对不符合严格企业规范的企业级与面向大众市场的智能设备加以区分。随着传统 IT 供应商的生态系统扩大到将运营技术和工业物联网供应商包括其中，采购活动的性质和采购文化将发生变化。

数据

首席信息官和首席数据官可能不得不考虑网络连接设备产生的数据和元数据的所有权。例如，法律允许何人复制、分发或创建以这些数据和元数据为基础的衍生作品？将由谁来施加控制？

与传统的联网设备和应用程序一样，确保数据隐私仍然是重中之重。根据《通用数据保护条例》（GDPR）、国际标准化组织、美国国家标准与技术研究院《网络安全框架》、《健康保险可携性和责任法案》、《美国联邦信息安全管理法案》以及其他行业和地方适用法规及准则收集并保护最终用户的数据是“入场筹码”。组织还必须考虑到，基于传感器和摄像头的设备通常会持续地收集和共享数据，有时最终用户并没有明确知晓这一点，或者并未得到其同意。例如，根据 GDPR 规定，可用于识别活人的静态或视频图像构成个人数据，应相应进行收集和保护。[9]

安全

保障这些实体资产的安全可能具有挑战性，因为它们通常是使用专有操作系统和通信协议开发的，内置安全性较弱，而且设备内存和计算能力有限。[10] 近期一项针对一百多万台企业和医疗保健物联网设备开展的分析发现，其中 98% 的设备流量都未加密，57% 的设备容易受到严重程度为中或高的攻击。[11]置于企业防火墙之外的业务关键资产构成了新的安全威胁，尤其是在嵌入了数据、机器学习算法和其他知识产权时。

方式与云和其他网络设备及端点通信、加密数据，并进行网络身份验证。大多数主要的云服务提供商都在其设备管理平台内置了安全防护功能，或者，可由 IT 部门开发和安装定制化安全保护工具，以确保所有设备都受到主动监控和保护。

设备采购过程中应就安全性和第三方数据访问两方面进行考量。要明智地选择供应商。在某些物联网设备上，安全研究人员发现了隐藏的后门，可用于将信息发回给制造商。[12]

产品工程服务：智能互联产品的研发

随着技术堆栈迈向实体化，产品研发也必然会从专注于独立产品（扬声器、恒温器和汽车）转向具有灵活消费模式，以及需要实时传输和分析数据的智能互联平台（基于云服务播放音乐的扬声器、具有自动调节设置并可通过应用程序进行控制的恒温器，以及可实现远程诊断、服务和升级的汽车）。此类产品非常复杂，往往需要同时改造业务模式、IT 系统和功能以及业务流程。

产品工程服务，或称 PES，是创造这些复杂产品的综合过程，包括从概念设计到软件和硬件开发再到制造等多个环节。举例而言，PES 范围可覆盖开发和集成 CPU 或 GPU 等硬件组件；操作系统、设备驱动程序和其他用于操作硬件的固件及嵌入式软件；以及提供特性、功能和用户界面的应用软件。另一项关键的 PES 活动是将智能产品连接到企业 IT 系统或基于云的平台，以跟踪消费并进行结算开票、监控业绩、收集分析结果。最后，PES 帮助产品团队利用由第三方供应商与合作伙伴构成的资源丰富的生态系统，可能需要借这些供应商与合作伙伴之力来制造或监控传感器和其他硬件，并开发用于应用商店、电子商务网站和其他分销渠道的应用程序。

必须掌握新的专业知识和技能组合

随着实体资产发展成为具有业务关键性并位于传统企业边界之外，可能需要掌握新的技能组合以对其进行管理、维护和监控。

例如，IT 组织可能需要在设备和网络中构建重要的技术、安全和弹性需求：可能需要电气工程师来开发传感器；需要能够对低功耗电子设备进行编程的系统工程师来执行信号处理、传感器调节和通信协议等任务；或者需要懂得无线电频谱管理的工程师来协助开展无线网络规划、分析、设计和优化工作。就工业企业生产设备而言，可能需要将基于传感器的联网设备和仪器与传统的制造系统、工业应用以及指挥、控制和监控系统进行整合。

将需要数据科学家、人工智能和机器学习工程师，包括那些专门从事视频和图像分析工作的工程师，来帮助组织管理数据、获得洞察力、实现决策流程自动化以及训练算法和模型。还需要其他专家来解决围绕数据采集、存储、交换、隐私和保护以及所有权产生的问题。

除了通常应具备的管理技能和软技能外，IT 项目经理可能需要对设备安全、运营和工业生产流程、变更管理以及终端用户培训有更多的了解。

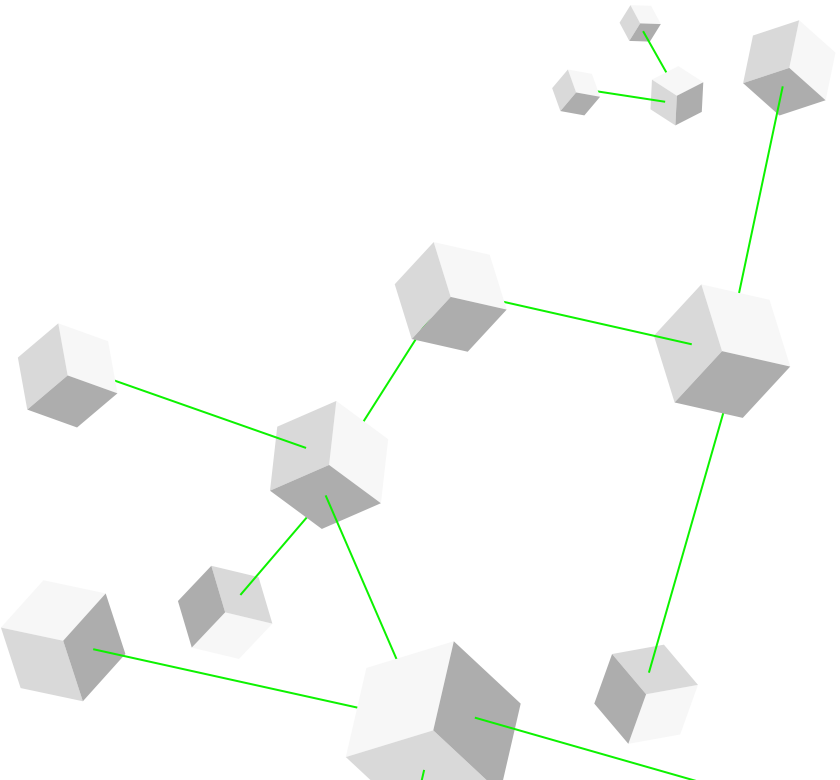
首席信息官们需要考虑是将业务外包，还是从零开始组建技能娴熟且专业水平高的内部团队。要重新培养现有的业务和技术人才，组织可以考虑培训外包，或创建内部能力中心和培训学院。

未来的方向

扩大的实体技术堆栈有可能极大地改变公司创造和交付价值的方式。由于具备了运用行业洞察力并通过人机交互促进收入增长的能力，各公司的商业模式可能会不断发展演变。例如，一家公司可能会将设备的监控和维护业务作为设备部署的附加服务项进行出售；可能会开发一种共享资产模式，在该模式下，客户将多余产能放回市场继续售卖；可能会利用传感器开发一款用于自动重新订购打印机墨盒等耗材的程序；可能从经销商模式扩展到直接面向消费者的模式；或者将其设备数据货币化。示例繁多，不胜枚举。

企业领导者可能需要衡量新兴实体技术堆栈对各个业务领域的影响。需要仔细考虑商业案例，尤其是针对拥有大量廉价设备的情况。在某些情况下，进行设备管理和维护的成本可能会超过潜在回报，即使仅需在廉价设备发生故障时将其更换也是如此。

这些嵌入传感器、由数据驱动的资产往往对业务至关重要。IT 部门可能需要确保其具有最高水平的弹性，升级无线网络和边缘计算功能以满足严格的延迟和吞吐量要求，并熟悉可能适用于新设备的新兴资产管理和管控要求。最后，首席信息官们可能需要重新考虑如何组建、定义、管理和培训技术队伍。为了挖掘所需的技术技能，首席信息官将不得不考虑是否重新培养和培训现有的人才，雇用新的技术工作者，还是将相关业务外包给具备相应技能的人员。



先行者经验

远大前景：物联网如何赋予航空业数据更清晰的含义

美国西南航空公司以专注于为客户提供优质服务而著称，长期以来一直在收集客户购票、值机和登机方面的事务处理数据，以不断提升旅客出行体验，改进运营流程。但是，当该航空公司将事务处理数据汇总起来后，发现了一个数据缺口：由于许多交互都发生在事务处理系统之外，它们没有被记录下来，也无法被衡量。

为了填补这个漏洞，西南航空公司开始尝试使用物联网（IoT）。该航空公司最早试水的项目旨在想办法节省飞机周转时间，即乘客下飞机、完成飞机起飞前的准备工作以及为下一班飞机安排乘客登机所需的时间。从七年前开始，西南航空公司试行了一项计划，在登机道上使用摄影机并利用计算机视觉技术来缩短飞机载客时间，同时确保客户隐私安全。自那时起，该航空公司继续试验并摸索物联网的应用，以改善旅客出行体验，提高资产利用率和机队管理水平，提升运营和维护质量。在旅客运程方面，西南航空测试了蓝牙和 Wi-Fi 信标的使用，以查看旅客在机场内聚集在何处，从而估算安检等待时间。在测试期间，如果旅客通过西南航空的移动应用程序选用了这项服务，当用户在整个机场范围内移动时，该系统将对用户的手机进行追踪并发送回显信息。

这凸显了先进的机器学习与物理基础设施相结合的方式，为以前不切实际的应用的推广提供了动力。然而，西南航空数据科学和自动化主管 Justin Bundick 表示，除了实现新的用例之外，这一趋势还有助于技术团队管理不断发展的实体基础设施，这需要新的技能、更长的正常运行时间以及更大的可靠性。[13]

Bundick 说，在建设物联网基础设施时，要解决的最重要问题之一是管理复杂的“多对多关系”。传统的 IT 基础设施需要补充各种实体设备和算法以支持一系列用例，物联网基础设施亦然：

“你必须确保它不是铁板一块，而是可扩展的，并且你正在与合适的 IT 基础设施供应商合作，从而确保一定的弹性。”[14]

西南航空公司团队的另一项重要学习任务是围绕测试进行的。虽然开发人员修复数字系统不会受到地域限制，但修复实体基础设施要复杂得多，特别是在机场这样对安全有着高要求的环境中。出于这个原因，西南航空公司投入生产的任何东西都需要是稳定可靠的，西南航空公司新兴趋势顾问 Kevin Kleist 如是说：“在真实环境中进行测试，使我们有机会更多地了解特定解决方案的可行性，同时也能获得关键的洞察并了解风险。”[15]

要正确应用物联网，需要广泛的人才和技能组合。例如，需要设备工程师来帮我们了解安装的设备，还需要网络安全专家来减少设备上的特殊漏洞。此外，Bundick 指出，重要的是要记住，“除非有数据科学家来分析数据，否则物联网设备产生的数据只是一大堆比特和字节。”

美国西南航空公司业务转型总监 Angela Marano 表示，她的团队一直认为，评估数据能为哪些领域带来独特价值，以及在哪些领域与供应商合作是有意义的，是非常重要的。她的团队需要解决新问题时，Angela Marano 就会评估团队拥有哪些技能、数据或能力可以使团队创造出比现有商业产品更好的东西。有时候团队的确拥有所需的技能、数据或能力，而有些时候，采用现成的成熟方案会更好。

Marano 说：“如今，我们在冒险和务实方面取得了良好的平衡。换句话说，这对企业有什么实际影响呢？我们必须确保我们真正了解自己在哪些方面拥有真正的竞争优势。”[16]

无人机彻底颠覆了电气基础设施的检查

南加州爱迪生公司（SCE）是利用无人机检查电气基础设施的先驱。该公司在约5万平方英里的服务区域内利用无人机确认电杆、线路、塔架、变压器和其他配电和输电设施的完整性。与直升机相比，无人机更加安全轻便，机动性和成本效益也更高，有助于SCE的机组成员快速完成检查和收集更准确的数据。在高野火风险区域，无人机的这些优势会更加突出。

2021年，约20万台位于野火风险区域的设施中有75%的设施采用无人机进行检查，数量比2020年增加25%。促使这一数量增加的原因在于无人机检查更彻底、更快、更准确。SCE检查主管Vibhu Kaushik表示："无人机可以比直升机更靠近设施，能够多角度、多视角拍摄设施照片。[17]我们获得了更近、更多、且质量更好的照片。这使我们更有能力掌握潜在设备问题、植被危害和其他起火风险。"

他继续说道："此外，在无人机的帮助下，我们能检查更多的设施，这比使用直升机更划算。雇佣无人机飞行员或培训操纵无人机的检查员也更容易。"

无人机检查计划的快速扩张给SCE带来了各种关乎增长的挑战和机遇。例如，检查员最初需要将图像存储在笔记本电脑上。随着高清图像的数量迅速增加，笔记本电脑存储不下这些图像。SCE随后迁移到云平台，现场拍摄的图像现在可由两名无人机机组成员直接传输到云端，供内部检查员查看和评估。

Kaushik 的团队目前正在测试一个让检查员自行训练驾驶无人机的改进流程。在检查员主导的无人机团队展开检查时，图像可存储到云端，并在平板电脑上接受现场评估。无人机飞行可以使用 GPS 坐标进行预编程，因此，检查员能够集中精力评估图像。

图像收集量太大也带来了额外挑战。SCE的服务区内有约140万个配电杆和14万台输电设施。每台设施检查需要拍摄10到12张图像；检查较大的输电塔则需拍摄400到600张图像。Kaushik指出："展望未来，每一张图像都需要人类检察员审查是不可持续的。"

Kaushik指出："展望未来，每一张图像都需要人类检察员审查是不可持续的。"为了突破图像瓶颈，SCE目前正在开发训练用于识别公用电杆、绝缘子和变压器等设施缺陷的人工智能模型。该公司为模型提供了数千张照片，使模型能够自动定位需要修复的设施。模型将作为图像检查评估的第一步，并在检测到异常时通知人类检查员。Kaushik解释到："人类检查员不需要检查数百万张图像，而是可以优先考虑被认定为有缺陷或可能有缺陷的图像。如此一来，我们就能更快地找到和修复有缺陷的设施。"

Kaushik指出，该公司人工智能模型正在逐渐成熟，已经能够达到较好的真阳性和真阴性成功率。

客户的认识和接受程度也是无人机检查面临的挑战。SCE制定了全面的社区推广计划，并与当地执法机构合作，对社区成员展开宣教。Kaushik 表示："我们也了解到自身品牌的重要性。与 SCE 的联系不明显时，客户的接受度会更低。"考希克说。但是当我们利用 SCE 品牌积极树立社区意识时，人们的态度通常是积极的，他们乐于接受这一新事物。"

为继续取得进步，SCE 正在扩大无人机的使用范围，将无人机用于检查大坝和其他发电设施，并协助维护和修理人员调查和修复损坏的设施。Kaushik 说："SCE 致力于利用无人机来提高电网的韧性、安全性和效率。无人机和智能传感器等技术正帮助我们建立起未来的能源网络，即低碳化、分布式、去中心化和自动化的能源网络。"

希巴医疗中心（Sheba Medical Center）制定智能医院标准

以色列希巴医疗中心多年来一直是全球最好的医院之一，部分原因在于该医疗中心采用了智能设备和其他数字技术。[18]该医疗中心总部位于拉马特甘，每年治疗近 200 万名患者，另有 75 个为中心内部的临床医生和医疗保健初创企业设立的研究实验室和 ARC（加速、再设计、协作）创新项目。

希巴医疗中心正引领利用传感器和摄像头的远程医疗、CT 扫描诊断人工智能及其他医疗保健领域的创新，以期提高患者护理水平。[19]例如，在许多智能医院还在设法解决警报疲劳（医生对大量的医疗设备电子提示和通知应接不暇）时，希巴医疗中心已经开发了技术集成方法，在提高质量、安全和效率的同时，却不会分散医务人员的注意力。希巴医疗中心首席创新官 Eyal Zimlichman 博士表示：“智能医院应该利用人工智能和智能设备来帮助医生提高效率，而不是剥夺他们的自主性。”[20]

希巴医疗中心为重症监护室（ICU）提供了基于人工智能的决策支持，帮助医生在数据密集而不确定性高的环境中处理复杂而关键的患者问题。重症监护室内的动脉压传感器等患者传感器产生大量数据，数据由希巴医疗中心的人工智能平台进行分析，为医生提供关键警报和护理建议。在高风险性环境中，医护人员可能由于缺少正确洞察而犯错。Zimlichman 谈到：“重症监护室内的每一项决策都会对患者健康和医院效率产生极大影响，因此我们将决策支持重点放在降低重症监护室的风险方面。”

希巴医疗中心还利用人工智能和医院设备产生的数据来解决运营问题。任何医院的管理者都需要指导活动和患者的流动，但他们往往不是基于数据做决策的。希巴医疗中心的团队正与多家初创企业共同开发一个控制塔应用程序，利用实时病床数据最大限度提高手术台分配和病人分配的效率。该团队目前也在研究持续护理应用，利用智能手表等可穿戴技术监测慢性病患者。Zimlichman 表示：“通过建立满足患者需求的数字环境，我们可以对传统方法进行补充，减少住院数量。”

目前，ARC 团队正致力于为医生提供术中 AI 视频分析，以便外科医生能知道他们是否在正确的位置上切开了切口或者患者出血量是否超过安全阈值。随着这项技术改进，最终手术机器人将能从打开患者腹部等（相对）简单的任务开始独立进行手术。Zimlichman认为，未来 10 到 20 年内，机器人将能够承担最复杂的手术程序，甚至是远程手术。Zimlichman 谈道：“未来，机器人将完成 95% 的手术过程，就像飞机自动驾驶仪一样。外科医生只需监测和执行剩下 5% 的手术过程。”

医院目前是产生医疗成本的主要因素，但是希巴医疗中心已经证明，技术进步可以提高医院的先进性、高效性和安全性。Zimlichman 认为，随着技术继续进步，技术将使医生在医院之外也能够护理大多数病人，因此医院发挥的作用可能会减小，医院本身的规模也会变小。Zimlichman 说：“新冠疫情加速了医院变革，我们将在有生之年看到一片新的景象。”

我的观点

Brad Chedister

国防工场 (DEFENSEWERX) 首席技术与创新官

越来越多组织借助联网设备提供崭新和更好的服务和产品。

组织利用无人机系统 (UAS) 进行派送物品、检查铁路和执行侦察任务。工厂、快餐店、医院、国防机构等组织已经在利用机器人设备实现流程自动化，提高效率和交付水平。但在智能、互联网和自动化组织的时代，我们永远不应该忘记，人比硬件重要得多。

国防工场的技术开发和创新举措旨在帮助国防机构解决难题。我们的多个创新中心遍布美国各地，用来培育创新生态系统，帮我们制定保护国家的解决方案。在工作中，我观察到，随着组织变得更加数据驱动和设备驱动，挑战往往出现在人与技术的交汇处。

例如，当拥有遗留系统和工艺专业知识的组织不得不向新的技术和新的工作方式转变时，劳动力发展的重要性不言而喻。但有时，文化转变也是组织所需的。制定创新举措时，有些人可能会在一开始就认为“我们做不到，因为……”例如，我们做不到，因为这项举措与遗留系统不具备互操作性，或者部署和实施举措需要的时间太长。

我鼓励团队从“我们做不到，因为……”向“如果我们做得到，该怎么做？”转变思维。例如，如果我们可以开发出一种自动化 CRM 工具，能从超过85,000项创新的生态系统中筛选出新型工具去解决作战人员的问题，我们该怎么做？如果没有这种思维和随之产生的文化，智能自动化工具和系统可能永远会停留在起点。

这种文化转变能帮组织找到具有创新者所需技术技能的人才。组织要做的不仅仅是要与时俱进；还必须吸引未来的劳动力，即具备技术技能，能利用无人机系统和其他无人驾驶车辆、机器人、传感器、人工智能和机器学习、数据分析以及其他关键技术展开工作的人才。

有关人和技术（尤其是私营企业的自动化和机器人技术）的另一项挑战是，认为技术会剥夺人的工作的想法。国防工业中，我们最重要的资产是作战人员，不是装备或技术，因此我们的关注重点是要利用技术保护我们的人民。

例如，使用无人机侦察未知领土时，其实我们是在防止士兵受到伤害。事实证明，具有智能、监视、侦察软件和短波红外图像能力的无人机可以“看到”的距离是人类的 10 倍，因此无人机也是一种增效工具。同样，企业可以考虑如何利用智能设备和自动化来完成通常由人类完成的危险任务，在此过程中，智能设备和自动化也许还能够提升效率或带来其他改进。

无论是在私营部门还是公共部门，有些活动都是人类固有的。一些任务需要建立信任，体验温暖，因此需要人际互动。这些任务永远不会被人工智能或机器人取代。但是，只要任务自动化和系统机器人化有助于持续提高工作场所的安全性和效率，这一取代趋势就不太可能会减缓。

高管视角

战略

首席执行官越来越关注技术驱动的客户体验，这种客户体验越来越需要IT和物理技术之间保持一致。物理技术需要不同的韧性标准。典型案例： 停运或故障的自动驾驶车辆可能给乘客和旁人带来很大风险。首席执行官应确认其团队有能力达到新的物理技术标准，尤其是在对人类安全至关重要的领域。首席执行官可以与IT部门领导者合作，确保物理技术文化优先考虑客户的安全、安保和便利。

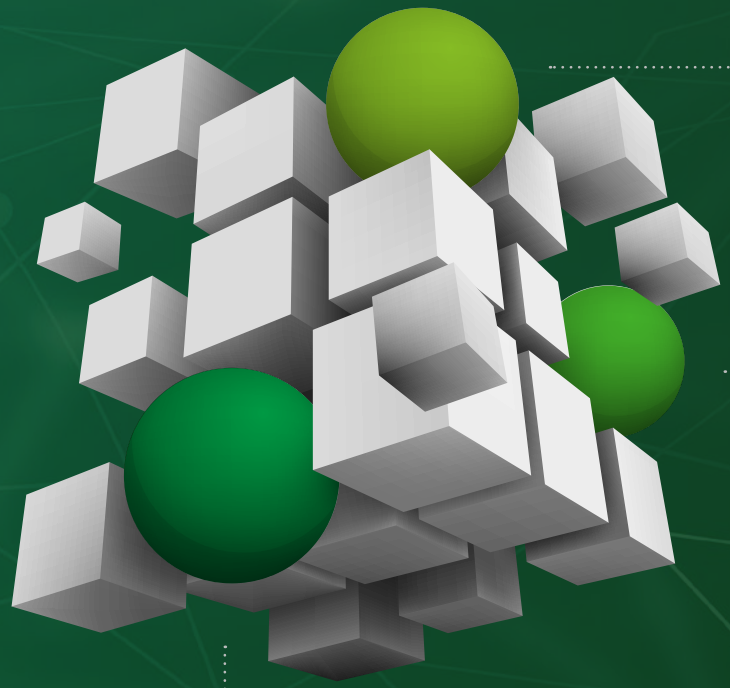
金融

由于智能设备变得如此重要，IT部门需要监督的设备越来越多。首席财务官应借此机会审查成本影响和风险敞口变化，包括出现故障或安全漏洞时可能对企业声誉或股东价值造成的损害。首席财务官可以帮助IT部门与风险、合规和其他职能部门展开跨职能协作。此外，首席财务官还可以审查企业的投资，以了解软件、硬件和物理技术的适当预算。

风险

虽然联网设备和 5G 网络等推动因素已经引起了大量关注，但多方面的相关详细安全要求仍处于定义阶段。随着医疗器械或工厂机器人等物理技术变得愈加关键，故障风险也急剧上升。首席风险官应与IT部门和和业务部门合作确定潜在的安全问题和相应的风险要求，也可以与首席执行官和首席信息官合作，强调可靠性，营造风险管理文化。

你准备好了吗?



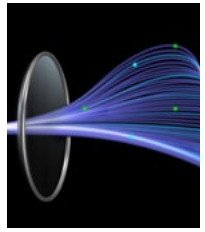
关键问题

1 如何加固技术基础设施，以提供维护新一代联网设备和实体资产所需的正常运行时间、冗余和安全？

2 哪些监管或合规授权可能会影响您管理日益复杂的实体资产？

3 需要哪些技能组合来管理、维护和保护数量、种类繁多的联网设备？您是否已经拥有这些技能组合，如果没有，您将如何获得这些技能组合？

了解更多



CXOs and 5G edge networks: Investing today for tomorrow's competitive advantage

投资当下，获得日后的竞争优势。了解5G边缘计算技术如何帮助组织获得下一阶段的创新、效率和敏捷性

Accelerating enterprise innovation and transformation with 5G and Wi-Fi 6

阅读德勤《先进无线应用研究（全球版）》，了解先进无线技术引起更多关注的详细情况。

Accelerating smart manufacturing

探索参与智能制造生态系统如何加快数字化转型和促进取得成果

作者

我们的洞察可以帮助你把握新兴趋势。如果你在寻找应对挑战的灵感，那我们可以谈一谈。

Peter Liu

无人机系统 (UAS) 及反无人机系统（CUAS) 技术负责人
德勤管理咨询
peteliu@deloitte.com

Robert Schmid

物联网业务负责人
德勤管理咨询
roschmid@deloitte.com

Sandeep Sharma, PhD

副首席技术官
德勤管理咨询
sandeepksharma@deloitte.com

资深撰稿人

Brian Greenberg
合伙人
德勤管理咨询

Britta Mittlefehldt
总监
勤管理咨询

Tim Paridaens
合伙人
Deloitte Belgium CVBA

Andreas Staffen
合伙人
德勤管理咨询

Thierry Cazenave
高级经理
德勤法国

Gabriel Goïc
高级经理
德勤法国

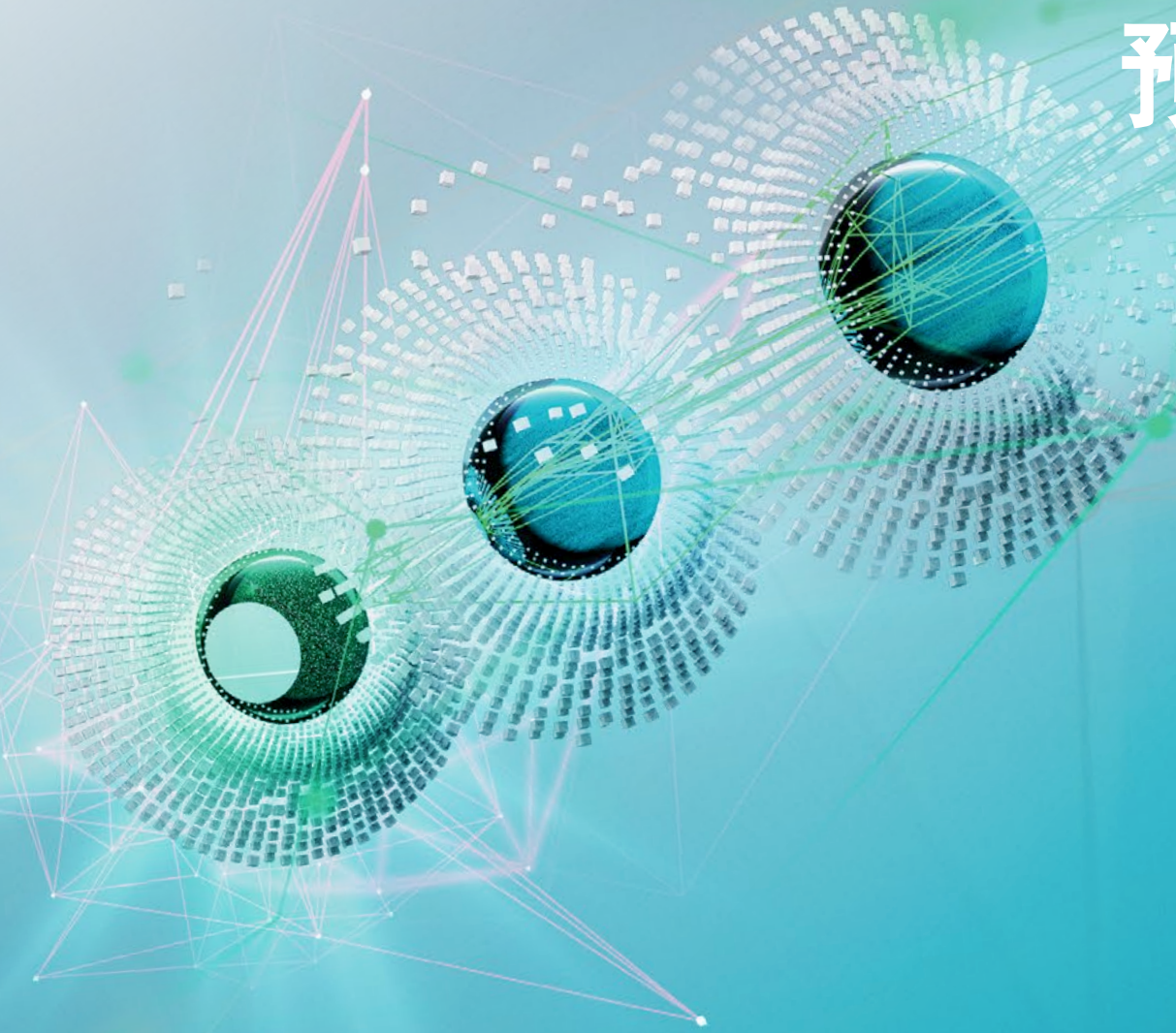
Adam Niedbała
经理
德勤波兰

Hugo Araujo
高级顾问
Deloitte MCS Limited

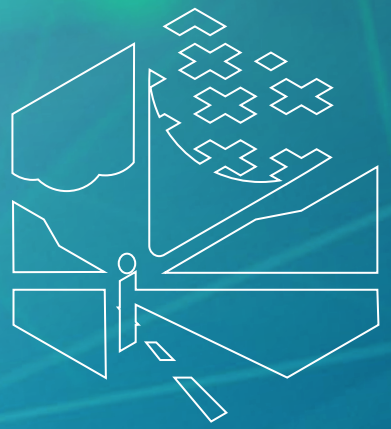
Nigel Forlemu
顾问
Deloitte MCS Limited

尾注

1. Gartner, Market guide for edge computing solutions for industrial IoT, accessed November 17, 2021.
2. Phil Marshall and Philippe Cases, Enabling the connected vehicle market to thrive, Topio Networks, accessed November 17, 2021.
3. Jack Fritz et al., Accelerating enterprise innovation and transformation with 5G and Wi-Fi 6, Deloitte Insights, March 22, 2021.
4. Intel, The edge outlook, accessed November 17, 2021.
5. Thomas Bittman, Bob Gill, Tim Zimmerman, Ted Friedman, Neil MacDonald, Karen Brown, *Predicts 2022: The Distributed Enterprise Drives Computing to the Edge*, Gartner, October 20, 2021.
6. The Linux Foundation, State of the Edge 2021: A Market and Ecosystem Report for Edge Computing, 2021.
7. Jaclyn Diaz,"U.S. announces new rules for drones and their operators," *NPR*, December 29, 2020.
8. IIHS,"Autonomous vehicle laws," accessed November 17, 2021.
9. University College London,"Guidance note on the use of images and videos under data protection law," accessed November 17, 2021.
10. Mary Shacklett,"IoT projects demand new skills from IT project managers," TechRepublic, July 14, 2021.
11. Palo Alto Networks, 2020 Unit 42 IoT threat report, March 10, 2020.
12. Internet of Business,"Security researchers find backdoor in Chinese IoT devices," accessed November 17, 2021.
13. Justin Bundick (director of data science and automation, Southwest), interview, September 8, 2021.
14. Ibid.
15. Kevin Kleist (emerging trends advisor, Southwest), interview, September 8, 2021.
16. Angela Marano (managing director of business transformation, Southwest), interview, September 8, 2021.
17. Vibhu Kaushik (director of inspections, Southern California Edison), phone interview with authors, October 22, 2021.
18. *Newsweek* editors,"The top 10 hospitals in the world," *Newsweek*, March 6, 2020.
19. Sheba Medical Center in Israel,"ARC – The center for digital innovation at Sheba Medical Center," accessed November 20, 2021.
20. Dr. Eyal Zimlichman (chief innovation officer at Sheba Medical Center), phone interview, November 11, 2021.



预判未来：来自未来的报道



量子技术及其他

量子研究将在未来十年内走向商业化。

指数级智能：再次感受

人工智能可识别人类情感。

环境体验：玻璃之外的生活

技术为所有人服务，无处不在。

趋势 7

预判未来：来自未来的报道

展望未来三大新兴技术

全球企业技术领域普遍持乐观态度。我们如此着迷于快速兴起的创新以及随之而来的充满机遇的变革，以至于我们有充分的理由对技术进步产生持久的信心。今日之橡实明日将成参天大树。或者说，人们偏爱这样的故事。

其中挑战在于，这类故事几乎总是大笔描绘乐观的结果。对于为下季度报表捏一把汗的的首席财务官而言，人工智能的快速发展将在五年内产生令人兴奋的新商业模式这一说法只是冷冰冰的安慰。

许多领导者、战略家和技术人员已经提出了合理的问题："我们目前可以做什么来应对性质和时间都不确定的未来事件？"我们的愚见是：如果你赌定，未来十年内，许多新兴技术将会促使令人兴奋的事情发生，那么，你很可能会赌赢。到底会发生什么呢？我们尚不清楚，也没有人清楚。但在《2022技术趋势报告》的最后一章中，我们确实提供了一个框架，为目前似乎刚出现在地平线上的技术的可能性进行战略角度思考。

我们重点讨论了三种我们认为值得注意的可能性：

- 量子技术有望在未来十年内改变计算、传感和通信
- 指数级智能是有望了解人类情感和意图的下一代人工智能技术
- 环境计算将使技术在我们的工作和家庭环境中实现普及

在展开讨论之后，我们也附上了德勤管理咨询首席未来主义学家 Mike Bechtel 所作的一篇回顾过去，展望未来的文章。

请继续读下去。

量子技术及其他

尽管量子计算正在迅速成熟，但它仍是许多深奥辩论的焦点。辩论焦点之一在于马约拉纳费米子是否存在。不可否认，大多数人与这场辩论毫不相干，但与之相关的人们似乎已经准备好要一辩究竟了。一些人认为，马约拉纳费米子粒子（理论上，该粒子的反粒子就是其本身）能够产生非常稳定的量子位。对此表示怀疑的人则认为，没有人能够找到证据证明马约拉纳费米子粒子存在。在此之前，马约拉纳的量子可能性仍然只是可能性。[1]
这场关于理论粒子的辩论某种程度上概括了当下量子计算的状态：尽管一切都非常有趣和富有前景，但我们仍处于量子技术的早期探索阶段。确切的时间表和研究突破仍在进行中。

然而，人们普遍认为，我们能把上述问题全部解决，并且，未来量子技术将对人类社会整体发挥巨大作用。事实上，量子研究势头正猛，预计未来十年内，实验室的研究成果将能够进入现实世界实现商用。[2] 技术巨头、政府和早期初创企业投资数十亿美元，旨在实现量子技术的突破。[3]

富有前景的重点领域包括：

- **计算**。量子计算机是解决先进计算问题的专用工具，利用量子现象处理信息和进行高度专业化的计算。考虑到这一点，量子计算机可能不会取代传统计算机，而是会与传统计算机共存，并根据复杂计算工作量的需要提供先

进的计算能力。[4] 最近的一些演示就展示了量子计算的潜力，在这些演示中，量子计算机在五分钟内完成了专门的任务，研究人员指出，这些任务需要传统超级计算机花费数千年的时间才能完成。[5]

- **通信**。量子通信是一种基于硬件的解决方案，利用量子力学原理创建理论上能够检测截获和窃听的防篡改通信网络。量子密钥分发 (QKD) 是达到这一安全通信水平的技术之一，是指通信各方通过交换高度安全的加密密钥在光网络间传输数据。尽管量子密钥分发技术尚未完全成熟，但已有多个量子通信网络部署完成或正在开发。[6]
- **感知**。由于亚原子粒子灵敏度高，量子感知装置比传统传感器响应速度快，准确度更高。未来十年，量子传感器很可能在某些应用中取代传统传感器。事实上，量子感知在能源、交通和医疗保健等领域都用很好的用例。量子传感器已经可以应用，但目前只在有限范围内应用。研究人员正在努力使量子传感器更便宜、更轻、更便携、更节能。[7]

虽然量子动力学面临着许多令人费解的挑战，但量子技术正在进步。随着量子动力学逐渐成熟，我们很容易会被有趣的技术细节所吸引。什么样的技术人员才能忍住不去思考激光冷冻粒子和低于外太空的温度之类的问题？同样，什么样的商业策略家会忽视围绕量子技术供应商上市的投资热情呢？

五年内，我们将会有更深入的了解。

虽然我们可能无法准确知道我们能共同将量子技术发展到何种程度，但我们了解其发展方向。好消息是，五年内，我们将会有更深入的了解。我们也许将能够使用有趣的机器来优化诸如计算、通信、感知甚至化学等领域。现在是你的组织需要开始考虑这一未来景象的时候了。如果你持观望态度，你可能就会在竞争对手获取竞争优势的时候，错失测试和尝试量子技术的关键机会。

指数级智能：再次感受

在数据挖掘的民间传说中，有一个关于啤酒和尿布的轶事，许多人认为这是能够说明人工智能传统状态的有效例子。正如故事所言，对超市交易的分析显示，商店通过将啤酒和尿布摆在一起，可以促进啤酒销售。你也许会问，尿布和啤酒销售之间有什么关系？一位姓名无从考证的数据科学家推测，妻子会要求丈夫在下班回家的路上顺便买尿布。丈夫们按要求买尿布时，就会认为，为了照顾穿尿布的小家伙，他们需要用啤酒来犒劳自己。[8]

除了养育孩子是件难事这一恒久不变的事实之外，这背后还有一个重要的教训：机器驱动的销售交易分析只能指出尿布和啤酒销售之间的因果关系，人们需要自行推断和解释促进啤酒销售的客户情绪和心理。换句话说，尽管人工智能强大的分析能力受到大肆吹捧，但人工智能一直无法区分有意义和无意义的统计性联系。

未来十年，这种情况也许会发生巨变。我们在之前的《技术趋势报告》中考察了“情感计算”或“情感人工智能”这一类新的人工智能解决方案如何规模化地为技术智商增加情商 (EQ)。[9] 随着创新者利用下一代深度学习技术来训练机器，识别和模仿人的魅力、情感等特征，未来十年，情感计算还将继续变化发展。而这些技术也将通过“符号化”和“连接主义”技术将演绎推理和逻辑推理能力嵌入人工智能和人工神经网络。很快，这些技术将能够像人脑一样揭示统计相关性，确定这种统计相关性是有意义的还是只是缺乏内在意义的支持数据的随机特征。换言之，机器将能像人类一样更好地欣赏世界，而不只是缺少上下文的0和1集合。

这代表着我们与机器智能关系的转变。20 世纪 50 年代人工智能领域出现以来，我们一直非常重视了解这项新奇技术能够实现和不能实现的方面。人工智能增强了我们从数据中提取洞察的能力，却从不会削弱人类认知和情绪至高无上的地位。然而，机器的影响和能力增长是指数级的。在我们寻求效率和洞察的过程中，我们正通过设计使机器具备一定的情绪敏锐性，这种情绪敏锐性正在逐渐瓦解传统的人机认知层次结构。

先驱研究人员目前正在以非常人性化的方式训练人工智能应用程序，使其既能实现广泛用途又能关注细节。例如，通过按顺序识别所提的问题，人工智能机器人能够像人一样与呼叫中心、餐厅和银行的客户展开互动。下一步也许就是建造带传感器的高级护理机器人，机器人可以区分在夜间从桌子上掉下来的灯和摔倒后需要帮助的人。未来十年，随着人工智能的直觉和情感能力得到发展，机器人可能可以开始承担教育家、作家、医生甚至首席信息官的工作。

我们相信，这一发展、训练、部署过程将在未来十年及以后的时间里继续快速推进。当下看来独特的人类事物也将越来越多地可以用代码序列表现出来。如果能够做到这一点，企业领导者最终将能够充分利用自动化，这将对价值链、商业模式和战略产生颠覆性影响。十年似乎很漫长，特别是对于那些忙于完成下一季度报告的决策者来说，更是如此。但指数级智能进步不会等着你。组织现在就应该开始从容易实现的方面入手，实现自动化了。

如何看待科幻小说家长期以来一直向我们描述的那个恐怖的、反乌托邦的世界呢？无需害怕。 事实是，软件始终是中立的，体现的是开发者的明确命令和隐性偏见。[10] 德勤未来主义学家与世界经济论坛合作发表了《技术未来：预测可能，把握未来》这一报告，其中详细阐述了未来的可能性和实现这些可能性的方法。[11] 关于人工智能的未来，作者写道："随着信息技术持续从'要求机器去计算什么'向"、'教会机器去辨别什么'演变，密切监控机器的'教学课程'对于组织、政府和监管机构而言将变得越来越重要。如何发展能体现我们明确公认的财务、社会和伦理价值观的人工智能呢？我们必须教好我们的'数字化下一代'，训练他们按我们说的做，而不一定要按我们的行事方式去做。"

环境体验：屏幕之外的生活

自 20 世纪 60 年代命令行接口出现后，似乎只有未来主义学家和科幻小说家才敢于去想象技术不是藏在屏幕后面，而是真正得到普及的世界。通过一块矩形玻璃屏获取计算机能力和访问互联网的认识已经成了大多数人的教条。

随着时间的推移，这些玻璃屏幕变小了很多，现在已经能装进我们口袋或握在我们手上了。甚至，在这些不断变小的屏幕背后，数字运算和网络技术已经变得成倍的强大和复杂，以至于我们开始不需要玻璃作为中介，就能直接与云计算对接。看看智能音箱。如今在使用智能科技的家庭中长大的孩子不会想到，除了通过"问一问房间"来了解天气预报外，还有其他方法。

环境计算一词涵盖了让用户可以随时随地接触数字现实的整个新兴技术领域。未来十年，环境计算将成为我们的标准模式，并因此迎来一个超越玻璃的生活时代。这种生活是什么样的呢？想想以下场景：

- **更顺畅**。回想一下你第一次见到台式电脑的情形。当时的台式电脑很可能还附带了一本纸质的大部头说明书。相比之下，当今的移动设备只需要一个本身就是数字应用程序的"快速启动"功能即可。虽然底层技术变得更加复杂，但用户体验却变得更加简单。环境技术有望进一步降低学习和使用新工具的困难，因为就像我们的孩子们让房间来播报天气预报一样，你只需要说话，或者做手势， 或者瞥一眼即可。你不再需要去计算机实验室或登录笔记本电脑，甚至不用查看移动设备。事实上，环境界面将处于等待状态，耐心地推断下一步需要做什么，并主动提供完成下一步工作的最有效方法。

  我们设想未来有大量技术持续监测我们的环境，协调一致地自动化（或者至少是简化）我们的工作和个人生活。当然，我们还会有一些安全和隐私问题需要解决。但是我们可以肯定地说，我们中的许多人（当然，还有我们的孩子）将会过上更加简单顺畅的生活。这样的生活将会唾手可得。

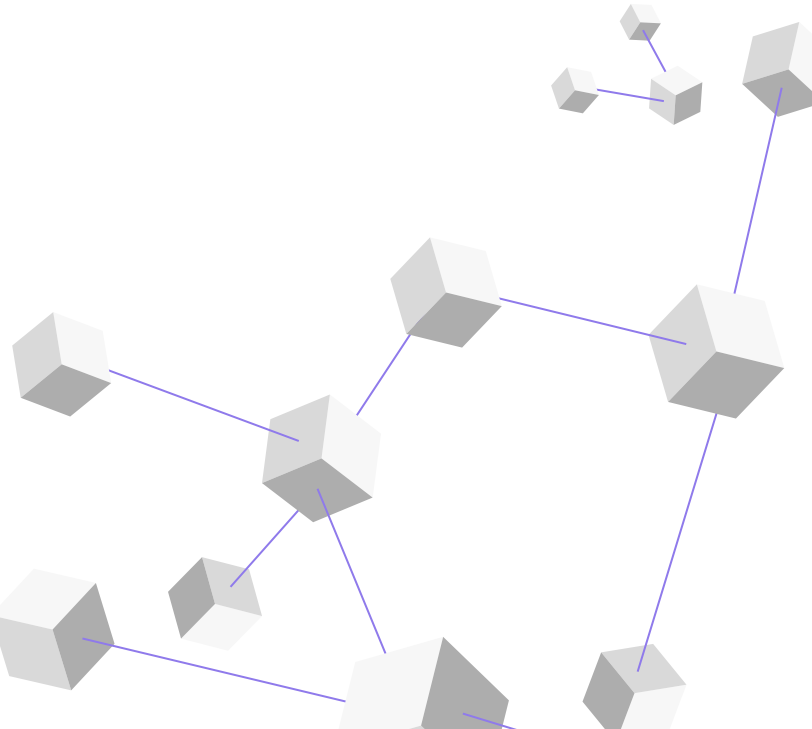
- **更主动、更直观**。想象一下，世界上每个人都有一位聪明无比、有能力又专注个人助理。这些高性能助理是数字化的，受到各类传感器、语音识别、分析和指数级智能能力的支持，能全天候监测环境，并尽可能减少用户会面临的困难。例如，数字助理可能会提醒你该去机场了。数字助理了解你的日程安排、喜好、意图，会替你完成全部所需工作，不需要再去确定你去机场的最佳路线，再在移动应用程序上进行值机。你拿起行李走出家门时，数字助理会关闭不必要设备的电源，将空调调节到最佳设置，再激活家庭安全系统。
- **眼睛看得到**。用数字信息增强个人的实际体验将是玻璃之外生活的另一个主要维度。我们已经看到最先采用相关技术的企业如何利用智能眼镜和虚拟现实或增强现实 (VR 或 AR) 耳机将数字信息叠加到工人的视野中。我们可以把这当作是将现实生活搬到线上，或者，也许是把位当做画笔来描绘原子，尽管这个画笔多少有些粗糙。相关研究人员和企业家都已经在探索利用智能隐形眼镜甚至通过植入脑芯片来增强人类感官和 (实实在在地) 读取人类想法的可能性。想一想： 通过观察太阳来确定距离日落还有多久难道不是自然而然的吗？或者，通过看公交站来知道下一辆公交还有多久到呢？我们固然很好奇，但也许，我们更喜欢整天盯着手机吧。

但是我们可以肯定地说，我们中的许多人（当然，还有我们的孩子）将会过上更加简单顺畅的生活。

前瞻性组织目前正重点关注容易实现的目标，同时稳步向更具变革性的项目迈进。在此背景下，我们将如何共同逐步创造出环境技术的世界呢？ 首先，先行者们已经在努力找出组织中现已存在的问题，其中可能包括人际交往、由来已久的繁琐流程，甚至是员工应用技术的方式。接下来，组织针对如何利用现有技术解决上述问题展开探索。航空业就是已经开始展开这类积极行动的例子。航空公司在过去十年通过数字化完全改变了客户体验，颠覆了从售票到行李处理，再到选座全部流程。这些变革目前仍在进行中，但是任何在过去二十年中曾经搭乘民航班机的人都不会否认，从取票到登机全过程的客户体验已经变得比过去更加简单了。零售、酒店和金融等其他许多行业也做了类似的努力。

对于客户和工人而言，“更容易” 也许实现所有环境技术目标所需的技术目前还没有，但很显然，它们很快就会出现了。

现在就开始玻璃之外的生活吧。



我的观点

Mike Bechtel

首席未来主义学家，德勤管理咨询

作为未来主义学家，我和我的团队花费了大量的时间研究过去。

我认为，我们是不为人知的历史学家。 具体而言，我们研究了各种技术的历史以及这些技术如何影响或未能影响世界的工作和生活方式。经过 25 年的创新研究，我们明白，预测单一的未来是无用的，而基于过去的模式预测各种可能的未来则可以帮助组织做到顺势而为，避开不利因素，更有意识地确定下一步的行动。

回顾 1840 年第一台计算机的专利，我们就能发现，其中的基本要素至今未变：交互（即用户界面），信息（即数据），计算（即中央处理器）。如本章所述，将这三个要素视为信息技术进步的基本因素，我们就能理解后续信息技术发展历程中的重要步骤可能什么样的了。超越移动设备和虚拟现实的交互催生了环境计算，使我们能够抛弃屏幕，体验数字世界和实体世界。信息带来了超越人工智能的指数级智能，在未来，机器可以学习如何拥有魅力，或者如何创作诗歌以及计算变量。最后，超越数字比特的计算产生了量子技术，使我们能应用物理学来解决数学难以解决的问题。

同样，正如内容创作已经实现民主化一样，信息技术方面的许多历史负担也消除了。数据库管理问题被抽象到云端，软件创建的障碍也被开源技术和代码加速器取代。未来IT组织可以用来相互连接的现成构件将更加丰富，证明组织内部自行创建构件具有合理性所需的应用程序将更少。结论是： 未来的IT团队更像是指挥家，而非作曲家，他们不会为有限的使用范围发明新的产品，而是整合现有产品的最佳配置。

IT领导者的职责也必须随着IT团队职责的变化而发展。随着技术不断激增，合适的工具变成了扶持性的背景，而非关键问题，首席信息官将日益将注意力转向信息而非技术。通过减少作为技术人员的时间，首席信息官可以腾出时间更深刻地了解自己的业务和市场。未来，首席信息官将成为首席执行官的得力助手，成为首席执行官的委托顾问，助其引导组织走向新的方向，展开下一步行动，以及进入应该投资的领域。

仰望星空，脚踏实地

要实现上述变革，IT团队需要下定决心，展开探索。否则，其团队所需的资源将被默认分配给运营团队。他们应该设置防火墙，并让5%到10%的团队成员专注于探索新的趋势，让15%到20%的团队成员致力于逐步实现最富有前景的创新。正如 Oren Harari 所说，“电灯并非是蜡烛不断改进而来的。”创造新“灯泡”的成本也许会高到令人望而却步，但其回报也是指数级的。如果组织能保持平衡，既优化现状，又能驱动新事物，那么他们就能实现期望的未来。

作者

我们的洞察可以帮助你把握新兴趋势的机遇。如果你在寻找应对挑战的灵感，那我们可以谈一谈。

Mike Bechtel

首席未来主义学家
德勤管理咨询
mibechtel@deloitte.com

Scott Buchholz

政府与公共服务首席技术官
德勤管理咨询
sbuchholz@deloitte.com

资深撰稿人

Doug McWhirter
高级经理
德勤管理咨询

Caroline Brown
经理
德勤管理咨询

Amy Golem
经理
德勤管理咨询

Raquel Buscaino
高级顾问
德勤管理咨询

Nelson Launer
高级顾问
德勤管理咨询

Abhijith Ravinutala
高级顾问
德勤管理咨询

Lucas Erb
顾问
德勤管理咨询

尾注

1. Sergey Frolov, Quantim computing’ s reproducibility crisis: Majorana fermions, *Nature*, April 12, 2021.
2. Scott Bucholz, Deborah Golden, and Caroline Brown, A business leader’ s guide to quantum technology, Deloitte Insights, April 15, 2021.
3. Daphne Leprince-Ringuet,“The global quantum computing race has begun. What will it take to win it?,” *ZDNet*, February 9, 2021.
4. Deloitte analysis.
5. Frank Arute et al.,“Quantum supremacy using a programmable superconducting processor,” Nature 574 (2019): pp. 505–10, Daniel Garisto,“Light-based quantum computer exceeds fastest classical supercomputers,” *Scientific American*, December 3, 2020.
6. Deloitte analysis.
7. Bucholz, Golden, and Brown, A business leader’ s guide to quantum technology.
8. Gregory Choi, Data mining: Association rules in R (diapers and beer), blog post, Data Science Central, August 22, 2016.
9. Tamara Cibenko, Amelia Dunlop, and Nelson Kunkel, *Human experience platforms:* Affective computing changes the rules of engagement, Deloitte Insights, January 15, 2021.
10. World Economic Forum, Technology futures: Projecting the possible, navigating what’ s next, April 5, 2021.
11. Ibid.

致谢

执行编辑

Scott Buchholz
新兴技术研究总监
政府与公共服务首席技术官
德勤管理咨
sbuchholz@deloitte.com

作为新兴技术的领导者和远见者，Scott Buchholz 帮助客户利用技术变革组织、使命和业务。他服务于各行各业，提供可行的建议和见解，利用技术提高性能、有效性和效率。

领导德勤管理咨询探索量子计算和相关技术，努力用这些先进技术解决客户面临的挑战。作为德勤管理咨询政府与公共服务实践的首席技术官，Scott Buchholz 与政府客户合作，利用技术创新运营、技术和任务交付。

Mike Bechtel
首席未来主义学家
德勤管理咨询
mibechtel@deloitte.com

作为德勤管理咨询的首席未来主义学家，Mike Bechtel 帮助客户制定战略，从而在面对业务中断和变革时仍能蓬勃发展。Bechtel 的团队研究了最可能影响企业未来的新的指数技术，并与创造这些技术的初创企业、领先企业和学术机构建立了关系。

加入德勤之前，Bechtel是早期风险投资公司Ringleader Ventures的高管，该公司是Bechtel 本人于2013年创立的。在此之前，Bechtel曾担任全国性非营利性组织Start Early 的首席技术官，该组织专注于危险青年的早期儿童教育。Bechtel的技术研发生涯始于一家全球性专业服务公司。任职期间，Bechtel的十几项美国专利帮助他成为公司的全球创新总监。目前，Bechtel 在圣母大学担任企业创新教授。

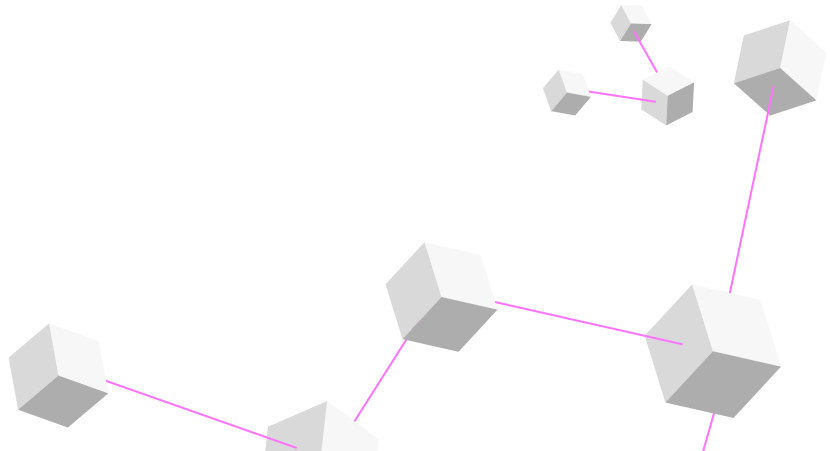
高管视角撰稿人

战略

Benjamin Finzi
美国与全球首席执行官项目 负责人
德勤管理咨询

Anh Nguyen Phillips
全球首席执行官项目” 研究总监 | Deloitte Touche Tohmatsu

Benjamin Stiller
战略负责人 | 德勤管理咨询



金融

Steve Gallucci
美国首席财务官项目 负责人 | 德勤管理咨询

Patricia Brown
美国首席财务官项目 总经理 | 德勤管理咨询

Ajit Kambil, PhD
首席财务官项目全球研究总监 | 德勤管理咨询

风险

Deborah Golden
美国网络战略风险负责人 | Deloitte & Touche LLP

撰稿人

Anthony Abbatista, Jaime Austin, Stefan Babel, Blair Baillio, Arod Balissa, Amod Bavare, Rupesh Bhat, Douglas Bourgeois, Tobias Brenner, Morgann Carlon, Natalie Chatterton, Anthony Ciarlo, Emily Cole, Morgan Davis, Louis DiLorenzo Jr., Greg Dost, Emma Downey, Michael Eniolade, Michael Fancher, Nairita Gangopadhyay, Andreas Gentner, Adarsh Gosu, Kevin Govender, Stefan Graf, Dorothea Haas, Esther Han, Ariana Hannes, David Harrison, Nikolaus Helbig, Michele Herron, Alexander Hewer, Meirav Hickry, Karen Johnson, Khalid Kark, Tim Kelly, Tovi Kochav, Kelly Komisar, Ed La Hoz Miranda, Matthias Lachmann, Amar Lakhtakia, Rebecca Lalez, Kristi Lamar, Bjoern Langmack, Louis Librandi, Mark Lillie, Daniel Martyniuk, Carey Miller, Simham Mulakaluri, Derek Nelson, Timo Perkola, Dalibor Petrovic, Felipe Piccirilo, Florian Ploner, Dilip Kumar Poddar, Vishal Prajapati, Aparna Prusty, Asish Ramchandran, Hannah Rapp, Alison Rogish, Daniel Rotem, Sanaa Saifi, Peter Sany, Heather Saxon, Rakinder Sembhi, Sofia Grace Sergi, Sandeep Sharma, Sandro Sicorello, Paul Kwan Hang Sin, Nitingaurav Singh, Ranjeet Singh, Nicholas Smith, Tim Smith, Ramona Stordeur, Jan Stratman, Elisabeth Sullivan, Natalie Velazquez, Markku Viitanen, Aman Vij, Jason Wainstein, Jian Wei, Denise Weiss, Shani Weitz, Sourabh Yaduvanshi, Thaddeus Zaharas, Yihong Zeng, and the Knowledge Services team.

研究团队

领导者

Emma Copsey, Ankush Dongre, Mayank Gupta, Rani Patel, Pooja Raj, Katrina Rudisel, and Samantha Topper.

团队成员

Ayshvar Balasubramanyam, Anupama Balla, Srinidhi Bapu, Niko Brammer, Yi-Hui Chang, Krishna Chanthanamuthu, Gurmehar Cheema, Hannah Chen, Soham Dasgupta, Francisco de Ros, Chirag Dixit, Chetana Gururaj, Nidhi Kaushik, Jonathan Key, Ashley King, Mo Koneshloo, Dhir Kothari, Sahil Lalwani, Dong Li, Antaryami Mallick, Swetha Marisetty, Siddhant Misra, Deepashree Mulay,
Rutuja Naik, Amruta Pawar, Anna Perdue, Harsh Raman, Vandhanaa Ramesh, Spandana Narasimha Reddy, Nikolaus Rentzke, Prateeti Sarker, Sai Krupan Seela,
Bala Seshu Sesham, Kshitij Pratap Singh, Manpreet Singh, Rachel Spurrier, Brendan Stec, Raghul Surendran, Jack Suter, Alap Trivedi, and Falyn Weiss.

特别鸣谢

感谢 **Stefanie Heng**，感谢您处变不惊，以及在领导技术趋势报告团队和管理公司时表现出的专业能力。如果不是您确保多项工作持续推进，我们的团队也许早已溃不成军。感谢您所做的一切！

感谢 **Doug McWhirter**。您拥有高度可靠的领导力和卓尔不群的智慧。您不仅听取中小型企业的声音，也培养了一批出类拔萃的摇滚明星设计师和作家。我们对您的赞赏之情无以言表。

感谢 **Caroline Brown**。您在面对压力时也能沉着冷静。我们感谢您在主导其他项目和指导团队成员的同时，还能基于意识流、研究范围和不耐烦的访谈撰写出精彩的文章。

感谢 **Adrian Espinoza**、**Ed Burns** 和 **Heather Mara**。你们在入职的第一年就表现出色。刚入职就承担技术趋势报告的工作绝非易事。你新颖的观点和想法已经巧妙地化为睿智的话语、漂亮的图表，以及令人信服而富有创造性的愿景。 非常棒！

感谢 **Natalie Martella**。感谢您抓住了每一个机会（以及每周通过讲笑话使我们感到轻松）。感谢您的指导。是您的帮助，使嘈杂的声音变成了一曲交响乐，并将其融入开发、设计和营销的方方面面。真好！

感谢 **Aaron Gano**、**Abhijith Ravinutala**、**Kelly Gaertner** 和 **Maria Wright** 在各方面所做的贡献。在不懈的研究、彻底的回顾、密集的访谈以及其他各项工作中，你们助力提升了标准（还给予了我们欢乐的氛围）。能与各位共事，我们非常幸运！

感谢 **Alison Cizowski**、**Cheylin Parker**、**Mary Hughes** 和**Tracey Parry** 为让《技术趋势报告》出版所做的不懈努力。感谢你们对包括营销、沟通和公关在内各项工作的支持！

感谢 **Aditi Rao**、**Andy Bayiates**、**Blythe Hurley**、**Sarah Jersild** 以及**整个德勤洞察团队**。感谢你们每年都能持续给予支持、保持耐心、展开合作，推动完善和改进《技术趋势报告》。

感谢 **Alexis Werbeck**、**Joanie Pearson**、**Mackenzie Odom**、**Matt Lennert** 和 **Green Dot 公司**。感谢你们在这一年里，再次展开了不起的合作，使我们的创造性愿景成为现实。我们正变得越来越好。

特别鸣谢

感谢**黄伟强**、**孟晓凡**、**刘俊龙**对《2022技术趋势》中文版发布工作组的悉心指导和支持，确保内容、培训、公关、市场活动各项工作朝着正确的方向推进。感谢**韩光辉**、**张志钢**、**陈颖思**、**王伟健**、**林暄**在报告编撰工作中的贡献和参与。

德勤管理咨询中国业务联系人

黄伟强
客户、行业和市场战略总裁
德勤管理咨询中国
woolfhuang@deloitte.com.hk

孟晓凡
企业技术与绩效事业群总裁
德勤管理咨询中国
denmeng@deloitte.com.cn

李伟杰
战略、数据分析与并购事业群总裁
德勤管理咨询中国
klee@deloitte.com.cn

华思远
客户与营销事业群总裁
德勤管理咨询中国
phua@deloitte.com.cn

龚戈亮
核心业务运营事业群总裁
德勤管理咨询中国
ggong@deloitte.com.cn

颜蓉
人力资本事业群总裁
德勤管理咨询中国
ramonayan@deloitte.com.cn

北京
北京市朝阳区针织路23号楼
国寿金融中心12层
邮政编码：100026
电话：+86 10 8520 7788
传真：+86 10 6508 8781

长沙
长沙市开福区芙蓉北路一段109号
华创国际广场3号栋20楼
邮政编码：410008
电话：+86 731 8522 8790
传真：+86 731 8522 8230

成都
成都市高新区交子大道365号
中海国际中心F座17层
邮政编码：610041
电话：+86 28 6789 8188
传真：+86 28 6317 3500

重庆
重庆市渝中区民族路188号
环球金融中心43层
邮政编码：400010
电话：+86 23 8823 1888
传真：+86 23 8857 0978

大连
大连市中山路147号
申贸大厦15楼
邮政编码：116011
电话：+86 411 8371 2888
传真：+86 411 8360 3297

广州
广州市珠江东路28号
越秀金融大厦26楼
邮政编码：510623
电话：+86 20 8396 9228
传真：+86 20 3888 0121

杭州
杭州市上城区飞云江路9号
赞成中心东楼1206室
邮政编码：310008
电话：+86 571 8972 7688
传真：+86 571 8779 7915

哈尔滨
哈尔滨市南岗区长江路368号
开发区管理大厦1618室
邮政编码：150090
电话：+86 451 8586 0060
传真：+86 451 8586 0056

合肥
安徽省合肥市蜀山区潜山路111号
华润大厦A座1506单元
邮政编码：230022
电话：+86 551 6585 5927
传真：+86 551 6585 5687

香港
香港金钟道88号
太古广场一座35楼
电话：+852 2852 1600
传真：+852 2541 1911

济南
济南市市中区二环南路6636号
中海广场28层2802-2804单元
邮政编码：250000
电话：+86 531 8973 5800
传真：+86 531 8973 5811

澳门
澳门殷皇子大马路43-53A号
澳门广场19楼H-L座
电话：+853 2871 2998
传真：+853 2871 3033

南昌
南昌市红谷滩区绿茵路129号
联发广场写字楼41层08-09室
邮政编码：330038
电话：+86 791 8387 1177

南京
南京市建邺区江东中路347号
国金中心办公楼一期40层
邮政编码：210019
电话：+86 25 5790 8880
传真：+86 25 8691 8776

宁波
宁波市海曙区和义路168号
万豪中心1702室
邮政编码: 315000
电话：+86 574 8768 3928
传真：+86 574 8707 4131

三亚
海南省三亚市吉阳区新风街279号
蓝海华庭 (三亚华夏保险中心) 16层
邮政编码：572099
电话：+86 898 8861 5558
传真：+86 898 8861 0723

上海
上海市延安东路222号
外滩中心30楼
邮政编码：200002
电话：+86 21 6141 8888
传真：+86 21 6335 0003

沈阳
沈阳市沈河区青年大街1-1号
沈阳市府恒隆广场办公楼1座
3605-3606单元
邮政编码：110063
电话：+86 24 6785 4068
传真：+86 24 6785 4067

深圳
深圳市深南东路5001号
华润大厦9楼
邮政编码：518010
电话：+86 755 8246 3255
传真：+86 755 8246 3186

苏州
苏州市工业园区苏绣路58号
苏州中心广场58幢A座24层
邮政编码：215021
电话: +86 512 6289 1238
传真: +86 512 6762 3338 / 3318

天津
天津市和平区南京路183号
天津世纪都会商厦45层
邮政编码：300051
电话：+86 22 2320 6688
传真：+86 22 8312 6099

武汉
武汉市江汉区建设大道568号
新世界国贸大厦49层01室
邮政编码：430000
电话：+86 27 8538 2222
传真：+86 27 8526 7032

厦门
厦门市思明区鹭江道8号
国际银行大厦26楼E单元
邮政编码：361001
电话：+86 592 2107 298
传真：+86 592 2107 259

西安
西安市高新区锦业路9号
绿地中心A座51层5104A室
邮政编码：710065
电话：+86 29 8114 0201
传真：+86 29 8114 0205

郑州
郑州市金水东路51号
楷林中心8座5A10
邮政编码：450018
电话：+86 371 8897 3700
传真：+86 371 8897 3710

Deloitte.
Insights

注册订阅德勤洞察最新资讯：www.deloitte.com/insights.

关注 @DeloitteInsight

www.deloitte.com/us/TechTrends

关注 @DeloitteOnTech

德勤洞察撰稿人

编者： Aditi Rao, Blythe Hurley, Andy Bayiates, Aparna Prusty, Dilip Kumar Poddar, Emma Downey, Nairita Gangopadhyay, and Rupesh Bhat

创意： Alexis Werbeck, Adrian Espinoza, Heather Mara, and Jaime Austin

推广: Hannah Rapp

封面插图设计: Bose Collins

CQ-007SC-22