# 扩展数字化规模

*构建安全、敏捷、高效的组织*

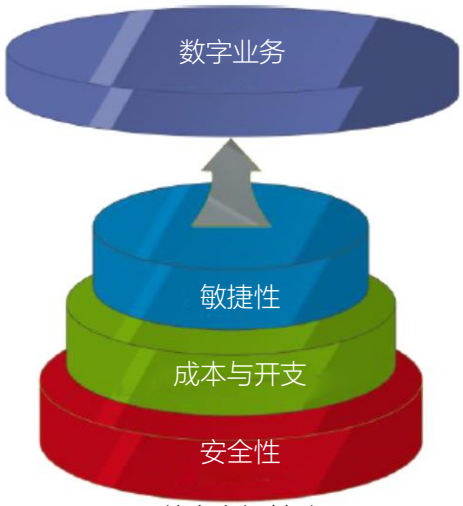
*"早在三年前，我们就认识到，如果我们想要我们的企业在 10 年后仍旧能够存续，我们就必须快速响应市场变化，并据此推动业务转型。我们的客户已经开始在线运营，因此我们也需要这样做。我觉得，如果我们不这样做的话，我们的企业将不会再成为一个年营收高达十亿美元的公司，而只会成为历史。我曾在董事会会议上说过，我们只有两条路可走，要么是迈上网络高速公路，实现更大发展，要么就会被颠覆、被淘汰。"*

某家国际零售集团公司的首席执行官，2018 年 2 月

## 引言

您是否希望您的企业在三年后仍旧能够存续？这个问题听起来好像很愚蠢，但却是目前存续的每一组织都面临的一个基本问题。推动业务转型、参与数字市场势在必行，而且就像一场赛跑。已经认识到新时代企业存在基础所在的组织已经开始把握这次机会，而其他组织则仍在犹豫不前。总而言之，组织及其客户必须确保安全，妥善保护交易，并确保数据安全。

在客户交互速度比较缓慢而且可控的时代，企业即便是每一年或每两年更新一次应用或服务产品，也不会出现多大问题。但这种时代已经一去不返。全球分散且不断扩展的市场催生了 24 小时可用性，这意味着更大数量的客户群体会产生不同的需求，而且这些需求有时还会存在冲突。



数字市场基础

对于希望赢得客户业务与忠诚度的每个组织而言，都面临着目标不断变化的问题。若要在竞争中立于不败之地，敏捷性有所欠缺的组织就必须调整对待创新的态度，并专注于构成客户群的每个消费者。

任何一个企业若要提升其在客户心中的分量，就必须进行持续创新，产品也要不断推陈出新。在许多最终消费者零售市场，客户会不断被频繁更新产品的组织所吸引；因此，如果某个组织在创新方面步伐缓慢、缺乏响应性，且仅仅针对同一客户需求，就会丧失之前在产品质量或广度上建立的优势。

在当今的市场环境下，客户忠诚度会呈一直下降的趋势。因此，每一天甚至是每个小时，企业都必须采取措施强化和稳固客户忠诚度。

这一竞争指标会推动灵活性以及市场对顶级业务需求的响应性的提升。因此，许多组织都在尝试将该指标纳入到成本高效且安全的商业界面中。对于适应性差的组织，如果尝试对组织进行重新架构，同时过度利用现有基础架构和组织程度，以期发挥它们的最大功能，会带来显著的负面影响，在某些情况下，甚至会导致完全失败。

在全球范围内的数字市场中，客户的获得与维系都需要创新性与敏捷性。如果没有这种响应性，组织就很难长久存续，也会轻易地在竞争中被淘汰。

## 数字转型

> *"我们用了 9 个月的时间实现了从'石器时代'到'摩登时代'的转变。"*
>
> David Giambruno，Tribune Media 高级副总裁兼首席信息官

转型列车已经启动，问题的关键在于您的组织能否登上这台列车。转型意味着对业务运营方式进行重大变革，而这就需要部署最好的工具并投入针对性的开支。在这个关键时刻，对拟纳入组织基础架构之中的各个组件进行谨慎评估尤为重要，因为整个商业世界都处在一片喧闹之中。

在此情况下，客户需求与产品之间的匹配性至关重要，但由于紧迫性的原因，也使得这种匹配变得更加复杂。那些所推出的产品或服务能够在这种演变过程中解决某些挑战的组织，已开始尽力去准确了解产品/服务如何才能以最佳的方式契合客户需求。

在不断增长的数字业务市场上，最首要的需求就是安全性。这里所说的安全性不仅包括组织数字资产的安全（如财务信息安全、数据处理完整性等），还包括客户信息的管理安全。融入基于 Web 的业务网络是实现产品与服务提供者与购买者之间信赖的基础所在。在数字业务方面，若想实现任何持续的客户忠诚度和成功，都必须以信赖为基础。

在日益数字化的业务格局中，另一条业务运营准则是确保组织响应市场需求的速度。无论是响应客户对新功能的需求，还是开放新市场，或是补救问题，作为数字市场参与者的企业都必须能够支持不断提升的速度。速度的内涵很广泛，从提高产品/服务上市速度，到确保组织灵活性，使得企业能够更好地改善程序和产品，实现与客户的高效沟通并为其提供一流服务，都属于速度的范畴。缓慢响应也能立足的时代已经一去不返。唯有那些能够快速采取行动并持续演变的组织，才能在当今的数字时代实现繁荣发展。

数字业务的第三个优先事项是确保开支的可控性。如果能够不断提升运营效率，同时能够在确保所需功能的前提下最大程度地降低成本，就称得上是注重成本节省的精益组织。无论是货物或服务的提供成本，还是确保资产安全所必需的开支，收支平衡仍旧是判断数字业务整体运行状况与生存力的关键。

组织若想通过数字转型提升竞争力，就需要协调各种变革，从多个变革因素着手同时发力。唯有奠定了坚实的基础，这种转型才会有意义。

# 安全 - 确保客户的信赖

*"网络信赖度对金融行业而言至为关键。安全与威胁之间的统一性是确保声誉与客户信赖的关键因素之一。"*

Stéphane Nappo，IBFS 全球首席信息安全官、顾问，法国巴黎

客户希望组织能够保护组织所收集并在业务开展中所使用信息的安全。如果组织无法做到这一点，组织的声誉很快就会受损，而且安全保护不到位对声誉的损害速度要远远快于其他任何因素。安全保护不到位实际上是违反了买卖双方所签订的合同。

如果客户认为某个组织存在违反合同的行为，那么客户再次与该组织进行交易的可能性微乎其微。一项针对 175,000 家组织进行的调研结果显示，超过 78% 的客户表示，如果某个组织在发生数据泄露后未能立即坦白承认，也没有详细地解释如何修复漏洞、补救损害，他们就肯定不会再次与该组织进行交易。超过 95% 的受访客户将组织在发生数据泄漏后试图掩盖泄露的行为视为不尊重客户的表现之一。正如某个受访者所说，"既然商家不拿我当人看，我为什么还要和他们做生意？对于根本不尊重我的商家，我为什么还要与其有纠葛？"

*"在遭到勒索软件攻击（sic）后，我们更换了大量服务器并耗费数百万美元恢复服务，但在不久之后，我们就遭到了第二次攻击。接二连三的攻击几乎让公司业务陷于瘫痪。对于一家金融公司而言，连续数天不营业是对公司声誉的极大破坏，而这种声誉是我们经过很长一段时间才建立起来的。我们耗费了数百万美元来挽回公司声誉，但估计成功的几率只有 75%。我们不仅在内部耗费了数百万美元来恢复服务，而且在外部，我们也耗费了数千万美元来唤回流失的客户。"*

某家中型金融服务公司的首席信息官

组织的生存力到底价值几何？35% 的客户流失会对公司利润带来怎样的影响？这些数据都是对认为网络安全保护麻烦大、浪费开支这一观点的有力回击。如果客户对某个组织失去了信赖，他们就不会再与该组织进行交易。

在过去数年里一直被新闻媒体广泛讨论的严重数据泄露事件已经证明了数字市场的危险性。不仅开展业务的组织会持续遭到攻击，而且一旦攻击取得成功，组织的智能资本和资产以及客户的信息都会面临风险。

我们已经跟踪了数据泄露对客户信赖及后续销售的影响，而且跟踪数据的分析结果显示，一旦发生重大侵入事件，平均客户流失率会达到 41% 以上。

这样一来，就会导致收入出现直接且持续的下降。此外，它还会进一步加剧已经受损的企业声誉。受各种补救因素的影响，这些流失的客户可能永远都不会再回来。若想挽回这部分客户，就需要在服务、设备和人员方面进行大量投入，重新获得客户的信赖。

在发生数据泄露后挽回客户所需的成本，最高可达到最初获得客户所需成本的 18.6 倍。在遭遇漏洞攻击之后，组织的任何市场拓展都离不开声誉重建，只有这样才能获得新客户的信赖。

换句话说，一旦遭受骇客的成功攻击，就会给组织业务带来非常严重的影响。

## 敏捷性 - 市场敏感性

*"现在已经过了'以大胜小'的时代，而是进入了'以快制慢'的时代。"*

Eric Pearson，International Hotel Group (IHG) 首席信息官

衡量组织在数字市场中成功与否的一个主要指标是组织应对不断变化的受众的能力。当市场格局发生变化时，通常都是第一时间作出响应的组织能够获得机会收益，即实现市场份额增加、收入提升。

随着数字混合体的日益移动化和分布化，给企业带来了新的复杂挑战。这些挑战带来的需求也非常多样化。这些需求涉及到许多领域，比如需要通过扩展解决活动数量剧增问题、建立安全机制来保护流程和数据、稳定性能以确保统一的响应时间，同时交付数据，以获取洞察力并实现个性化事务处理。

在这种环境下，基础架构的隐藏层和最佳实践至为关键。基础性的 IT 和业务选择比以往更为重要，尽管它们都不可见。这些特性的综合影响会形成一个综合性客户体验 (CX) 指标，而这个指标是获得市场份额、建立客户忠诚度的关键所在。

*"十年前，我们被称为一家创新型公司，因为每年会对我们的产品进行两次更新。现在，我们已经落后于竞争对手，因为我们需要 6 到 8 周才能推出新产品。我们收到的反馈信息是，客户认为我们已经无法跟上其他市场参与者的步伐。要么我们超过竞争对手，要么就会失去客户，这是一个非常迫切的问题。一旦我们失去了客户，就很难轻松地挽回他们。当今客户的看法都非常主观，而且非常快速，也非常关键。因此，我们展现自身创新素质的能力比以往任何时候都要重要。"*

某家大型保险公司的首席营销官

随着越来越多的商务以实时的方式进行，最终用户对 IT 基础架构的成效和效率的可视性也随之提升。一旦有应用出现质量瑕疵，很快就会体现到客户购买选择和市场份额上。无论是应用性能还是客户支持，如果出现响应速度慢的情况，就会引发长期性甚至是灾难性的后果。这不仅仅是对单次销售或单笔交易的影响，而且会左右客户对实际市场的反应。

服务交付质量可视性方面的变化，正在影响着组织对 IT 基础架构的选择。质量瑕疵越来越多地与收入流直接挂钩，而适当开支和成本的决定依据也在发生着巨大变化。这意味着，IT 基础架构的选择、配置及管理等方面正在发生着剧烈演变。运营结构正在重塑，因为业务支持过程中计算、存储、IT 人员配备之间的基础关系已经发生了变化。云部署与内部运营的复杂性也导致这种关系更加复杂化。

最终用户 CX 是两种完全不同的因素相结合的产物，这两个因素同等重要。从客户的角度来说，面向客户的应用的直观设计，以及交付这些应用的后端平台并非两个互不相干的方面。用户会将它们视作一个整体并从整体上进行评估。

一旦首席执行官意识到市场份额下滑或盈利能力下降，通常都会采取削减成本措施。不过，如果将 CX 考虑在内的话，在考量成本时，就必须考虑 CX 对市场预期的影响。在此之前，仅仅考虑一次性组件和廉价组件或许会是一个令人信服的商业案例，而现在系统可靠性对 CX 的影响就会轻易超过短期成本的影响。

除此之外还有许多因素会影响 CX，这些因素都与平台或应用无关。同时，这些因素也都是组织的网络空间中取得成功的关键。这些因素更多的是由组织态度和流程所决定，而不是计算机本身的相关因素。大概来说，这些因素包括：

- 最终用户对组织而言的重要性
- 每个客户对组织的看法
- 为最终用户提供个性化响应的灵活性

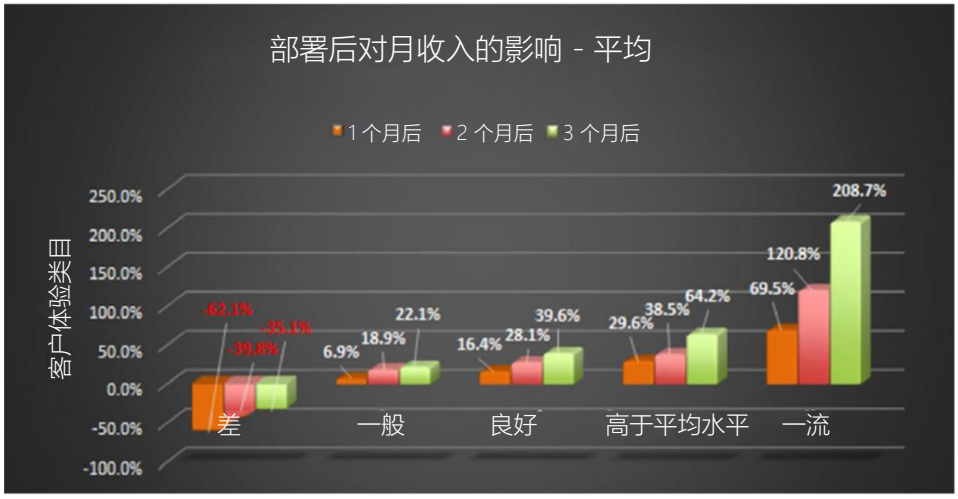

上述三个因素都与组织对待客户的态度有关。

潜藏的 IT 基础架构对业务的支持还可进一步进行细分。通过分层式的支持结构（包括应用和数据、运营环境和支持性 IT 基础架构），我们就可以建立竞争力、估值和生存力方面的针对性目标。

每个层次的要素都会对其他层带来正面或负面的影响。由于 CX 是各个层次综合作用的结果，因此我们不能简单地拉出某个组件来进行分析。任何一个组件都可能会产生连锁反应，进而对业务及客户交互的外围指标及 CX 带来重大影响。因此，无论是用于为客户提供操作界面的应用，还是用于进行快速信用决策的规则，又或是用于快速、统一地交付数据的硬件，所有的层次都非常关键。

CX 的基础在于以最终客户为中心，及时交付他们所需的内容。由于 CX 会给组织的净收入带来直接影响，因此越来越受到实际市场的关注。

通过下图我们就可以看出这种关注程度的提升，该图表针对的是在最近 6 个月内部署了新应用的 14,071 个站点。这些站点按照 CX 评级 (0-5) 进行了分组，对应于不同的体验水平（从差到一流）。从部署后的第一个月开始计算 CX 对月收入的平均影响量，从图示我们可以了解 CX 对组织现金流和净收入的影响。




我们根据第一个月的情况对影响量进行了平均，但影响量代表的是整体 CX 与收入之间的关系。从可实现次优体验的部署项目可以看出，相比客户体验更佳的部署项目，前者的收入级别永远无法成功回到之前的级别。

从下面两则客户引言可以看出客户体验两个极端完全不同的情况。

> *"我们的新零售产品在 7 个月前上线。我们在广告、开发和硬件方面投入了数百万美元。我们的营销部做得很好，成功地散播了新品发布的消息，一切都井然有序 ... 不过只维持了前三天的时间。*
>
> *在接下来的一周内，系统出现了 6 次宕机，至少有 6 个小时处于不可用状态。这给社交媒体及客户支持部门带来了非常严重的影响。据我们乐观估计，前三天所取得的成效都被所出现的问题完全抹杀。在我们找出问题之后，我们无法快速应对来解决问题。*
>
> *第一个月的收入甚至不到预期的 10%。更糟糕的是，我们在设备调遣、供应商及其他服务提供商协助方面还花费了超过 40 万美元。除此之外，我们还尽力向客户解释我们解决问题的方式，让他们相信我们并非无能为力，这方面又花费了 15 万美元。*
>
> *后续的销售情况非常糟糕，不足预期的 50%，因为我们没办法重新唤回客户。"*
>
> 某家大型零售商的首席运营官

初期的失利可通过成功、稳定部署所实现的优势来弥补。获得收入和新客户的机会是非常巨大的，而对竞争优势的渴求会迫使组织不断尝试，找出最适合自己的方法。

> *"我们大约在 9 个月前部署了一款新的销售产品应用。我们对部署团队的工作非常满意，而且在部署之后很少出现问题。新系统的市场反响非常好。现在，新系统的交易规模比预期高出了 60% 左右，并成为了我们盈利率最高的渠道。*

*目前，我们正在尝试每个月进行一些增量式变革和扩展，这无疑会有助于我们公司的稳定发展。客户反馈也都非常好，我觉得这次新系统的部署功不可没。"*

某家服务公司的业务线副总裁

上述两个示例曾多次在许多作为持续数据收集一部分的客户引言中使用，凸显了 CX 在组织取得成功方面的关键作用。CX 视图中的功能性、个人关注点和绩效要素会因为其他因素而放大，但最终都指向市场成功这一单个目标。

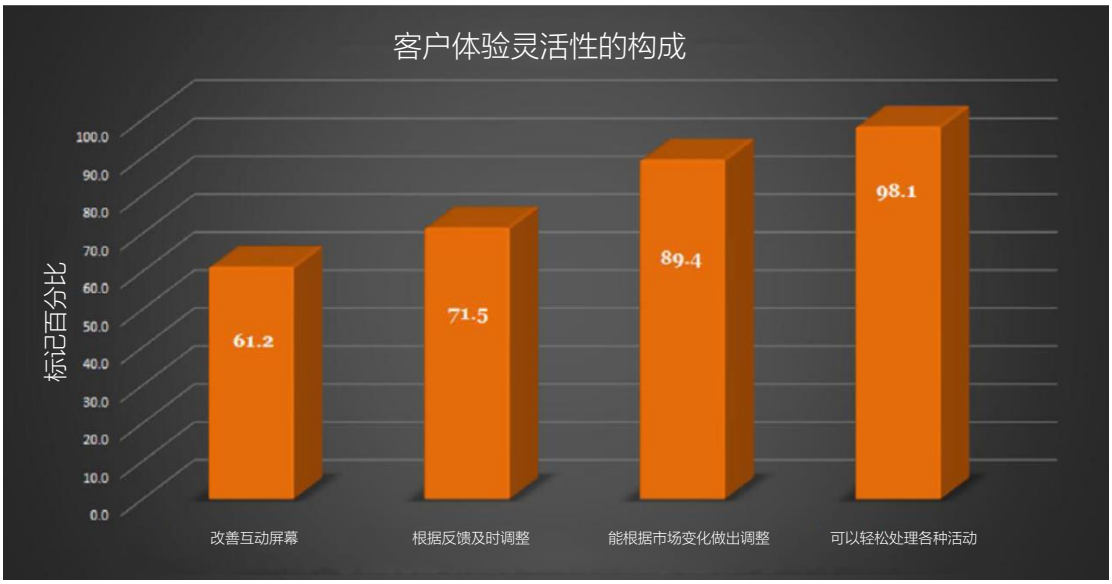
*"不是强者生存，也不是智者生存，而是适者生存。"*

Charles Darwin（1809 年 -1882 年）

市场需要灵活性。准确来说，灵活性是另一个混合性因素。针对全球各地的 140,000 个最终用户进行的数字市场期望调研结果显示，受访者都期望灵活性，但灵活性本身其实是被动要素和主动要素进行不同组合的结果。被动要素体现在组织愿意根据客户反馈调整用户界面、规则和流程。主动要素体现在组织会持续进行投入，为客户提供最新的"玩具"或流行元素。

尽管灵活性与速度密不可分，但灵活性的驱动因素并不仅仅只有速度。除了速度之外，还有两个主要方面。其一是对不断变化的产品的可视性。第二是交付的一致性。

如下图所示，组织在处理非预期负载（同时确保这些负载对用户不可见）方面的灵活性和弹性非常关键。通过类似于重复性客户交互的响应与交付机制，可以满足用户的基础性预期。此外，应尽可能地为客户提供便利，以免客户所期望服务或产品的交付出现不稳定或延迟的情况。一旦出现不一致的情况，就肯定会流失客户。



通过对客户反馈的分析我们发现，客户对灵活性的广泛期望是 CX 的关键，因此也是数字业务能够取得成功的关键。这对组织而言意味着，他们需要建立高度可调整的开发部门、可扩展的客户支持团队，同时构建弹性处理架构所需的基础。

对变化做出可视且快速的响应是这种高度敏捷数字市场的多变体制的一部分。客户反馈、法规调整、其他供应商互锁技术的变化或其他相关因素，都可能会导致应用和产品/服务的演变。对于组织而言，仅仅作出变革已然不够。他们还必须明确自己愿意对客户需求作出高效响应的态度。

这种可视性能够让客户感到他们与所交互的组织是相关的。单凭高效的文书工作或极具吸引力的实体店已经不再奏效，组织基于客户感知而与客户进行沟通的态度是确保客户粘性的关键。

或许在网络空间中传达这种观点具有一定的挑战性，但从其基本性质来看，这一点是组织完全无法避开的。

## 成本 - 运营效率

运营效率是指企业以最成本高效的方式向客户交付产品或服务，同时确保遵守高质量的标准。有些情况下，运营效率又被称作"有效开支"，即业务运营投入与业务收益之间的比率。一旦运营效率得到了改善，投入与收益之间的比例就会变得更加合理。该比率的计算一般基于资金（成本）、人员（员工数或全职员工当量）或时间与投入相当于收入的比例而得出。

由于数字业务极具动态性，会使这种计算变得复杂，这主要因为大多数组织都无法将商业行为与客户响应联系到一起。针对 19 万家组织进行的调研结果显示，只有 1.4% 的组织会采用正式的方法来关联商务与客户反应。这种关联的缺乏会导致组织内部难以分析潜在的改善领域，以及变革可能会对组织带来的收益。不过，如果不能很好地了解客户反应与收入流之间的关联，企业就会变得被动，而且在网络空间的持续商务运营过程中，就要耗费比所需资金更多的资金。

在对物理位置的依赖性降低的情况下，提升开支效率就会成为提升净收入的最有效方式之一。这也是组织在数字市场中最大的吸引点之一。如果组织不能抓住这种环境所提供的机会，就会落后于竞争对手。

## 网络空间战略

网络空间的风险趋势和范围仍在不断加剧，因此组织需要跟上步伐，在新的数字格局中开展运营，并抓住各种可能的机会。

对于许多组织而言，做到这一点存在着巨大的挑战。他们难以建立网络业务运营的稳定基础，要不断应对机器故障、安全泄露、性能不稳定等问题。这种问题不断的情况会耗费组织的精力和财力，并导致出现数十年来前所未有的业务波动。

通过尽职调查的新方式以及对快速市场响应的需求可以看出，组织当前所用的方法和态度并不足以应对数字市场环境日益严峻的形势。

从客户需求和业务风险的角度来说，组织急需进行变革。最终而言，这种变革的必要性可归结为一个问题，即：

*您是否希望您的企业在三年后仍旧能够存续？* 如果答案是肯定的，就表示您需要进行体制变革。若要实现这种变革，就需要组织能够灵活、及时地对市场变化做出应对，而这种需求也可以扩展为对成功数字业务的可变需求。

## 面向数字业务的解决方案

若要制定高效的组织路线，在严峻的网络空间环境中触达潜在客户，组织就要制定战略、克服挑战，这就需要组织充分了解需要纳入到数字业务之旅之中的不同组件。换言之，组织需要同时获取业务与安全方面的信息，并了解它们之间的交互方式。

对于能够支持并提升最优客户体验及数字业务水平的任何特定 IT 平台解决方案而言，都必须同时考虑技术和业务需求。由于平台选择对数字业务的影响与许多因素有关而且难以量化，因此 IBM 委托 Solitaire Interglobal Ltd. (SIL) 对 IBM LinuxONE 产品进行了客观评估。

为此目的，SIL 收集了 40 多年以来该领域市场演变及生产行为的相关数据。SIL 每年可为超过 6,000 多家客户提供支持并执行超过 1 亿次预测模型，而在最近 22 年，SIL 还提供全球安全观察 (GSW) 服务。通过这些会员服务，SIL 已经构建了一个非常详细的数据资料库，其规模已超过 550 PB。SIL 每个小时都会对这些数据进行挖掘，以进行趋势分析和对比，并找出有助于组织取得成功的阈值。

此外，SIL 还收集了许多额外数据来补充现有的数据资料库，同时进行了相关分析，以清晰地展现已部署了 IBM LinuxONE 的组织中效益与相对成本之间的关联。这些分析主要是从业务的角度来了解组织通过使用平台而带来的增量价值（正面价值和负面价值）。借助这些信息，业务领导者可以更好地了解 IT 平台对组织的收入及客户响应带来的影响。

数字业务与安全密不可分，因此任何分析都必须对这两者进行广泛关联。超过 22 年以来，SIL 一直都在致力于监控业务与安全的方方面面。该公司通过其"全球安全观察 (GSW)"收集的信息已经持续为数千家组织提供了趋势与风险相关信息。这种企业关键格局相关匿名数据的持续积累，多年来已为许多调研项目提供了丰富的数据基础。

近期的一项相关调研结果显示，市场对组织响应变革的需求，以及网络空间中活跃威胁的数量与规模，都在持续不断地增长。由于该领域的市场潜力越来越大，因此也越来越受到犯罪分子的"青睐"。无论是从受国家政府的指使、以影响其他国家/地区的稳定性为目的而实施的网络犯罪来看，还是从以更直接的金融收益为目的的网络犯罪来看，网络空间最终肯定会吸引众多企业加入其中，而企业同时也面临着巨大的风险。

GSW 是 SIL 推出的一项会员服务，数十年来，一直都在跟踪全球范围内安全威胁的详细演变过程，及其对业务的影响；到目前位置，已经从超过 121 万家组织收集到了大量数据。从业务的角度来说，通过 GSW 收集到的数据是一个广泛的威胁情报来源，可用作相关调研的依据，而且这些数据都是来自于真实的生产环境。尽管 GSW 也会收集威胁足迹及其他详细的机制信息，但其关注的重点在于对业务运营、组织资产及威胁防范和补救成本的影响。

借助客户体验反馈、IT 运营细节、业务绩效及安全等方面的相关数据，SIL 评估了 IBM LinuxONE 在数字业务市场中的定位。然后，SIL 将评估结果分成了三个领域，分别是安全、敏捷性和成本。之后，SIL 将这些领域融入到了在网络空间开展业务运营的组织认为最相关的主要目标之中。

## 安全和风险

部署项目中的风险与许多因素有关，但其中最重要的因素是成功侵入组织的系统和基础架构。防范此类侵入是数字业务安全人员的首要职责。

对于这些人员而言，任何损失都是不可接受的。每次数据泄露、规则违反或破坏防护层，都可能会带来灾难性的后果。网络攻击的数量每个小时都在不断增加，因此组织会频繁遭到持续的攻击尝试，这些攻击的目的包括破坏数据、盗取数据、妨碍他人使用商业服务等等。

在这场战争中，基础架构的基线特性至关重要，尤其是当基础性技术架构以提升骇客侵入难度为目的而设计时。

总体而言，骇客攻击是一种投机行为。就像盗贼会避开难度高的目标而选择更易的得手的受害者一样，许多骇客会选择攻击明显的目标。同时，随着越来越多的有组织犯罪出现在网络空间里，这种攻击的复杂性也在不断提升。对于此类犯罪分子而言，他们的攻击并非以容易得手的目标为主，而是选择能够为其带来最大价值的目标。此外，许多国家/地区也开始越来越多地参与数据盗窃和破坏活动，掀起秘而不宣的网络战争，这一因素又进一步增加了网络攻击的复杂性。这三种完全不同的网络犯罪因素进一步加剧了网络空间的复杂性，将其风险程度提升到了一个新高度。

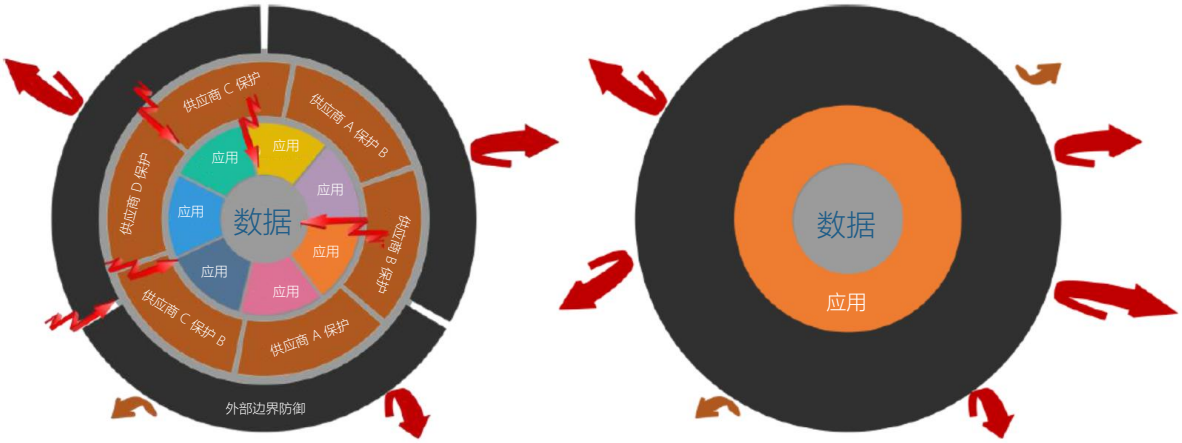
如果突破组织防线过于困难的话，骇客通常会转而攻击更易得手的"猎物"。此外，骇客社区会围绕新型高级工具和技术提供大量的增强攻击手段，比如有一种虚拟机器人，它可以强力攻击安全防护墙，寻求其中的保护弱点。通过上面的分析我们就可以看出架构的差异为何如此重要。

## 组合式安全与集成式安全拓扑

商业领域中许多可用的架构都采用组合式安全方法。每个组织可以选择如何装配自己的安全保护组件，也可以从大量安全产品/服务中随意挑选。

这种组合式安全方法的缺点在于，总是会出现许多传导点，各个保护组件通过这些传导点与其他不同的产品进行通信。由于这些传导点的独特性质，就会形成可被骇客利用的漏洞和机会。不过，这是这种设计的固有缺陷，而且许多采用这种设计的组织还会大肆吹捧其所提供的"灵活性和多样化选择"。

与组合式安全方法相对应的是完全集成式堆栈。在这种数字构造中，连接点是结构化的，而非可选的。因此，连接点和薄弱点更少，进而会减少漏洞点的数量及易受攻击的逻辑面。




组合式安全　　集成式安全

LinuxONE 安全功能的成功就在于它实施的是集成式安全堆栈。它所实施的保护理念是让客户无需购买容易被侵入的组件，也不会在保护层上留下可被攻击者利用的漏洞。尽管这种方式无法确保万无一失，但的确可以大幅减少易受攻击面。

这种安全架构的有效性已经过许多客户的验证；SIL GSW 的记录显示，就部署 1,000 个应用的实施项目而言，LinuxONE 实施项目的成功安全侵入次数*不到其他平台的 0.01%*。

在本次调研中，我们仔细评估了大量实际客户系统（超过 1,300 万个）软件和硬件的主要行为特性。所有这些客户在其生产环境中部署了安全应用，但所采用的安全方法和机制却千差万别。其中有些组织需要支持信息安全方面的监管标准和行业标准（如 HIPAA、PCI、SOX 等）。来自客户报告的数据以及相关的海量实际数据都是非常宝贵的，因为它们有助于我们从实际的角度（而非理论的角度）去了解不同类型的安全方法对客户能够产生怎样的影响。

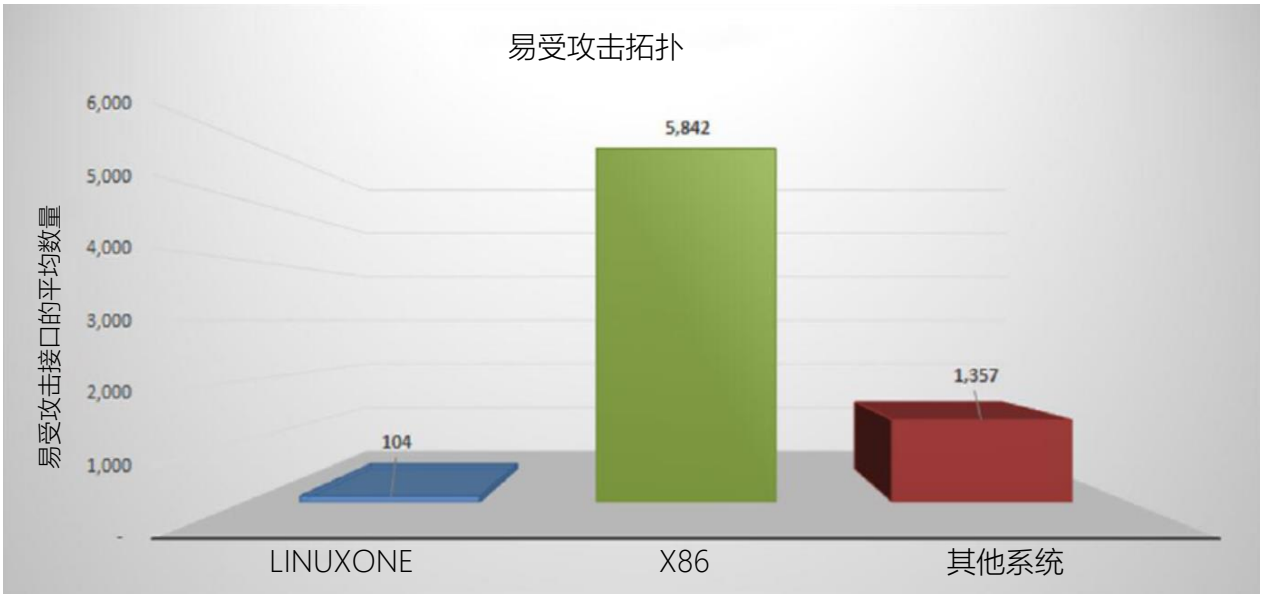
GSW 记录了针对详细侵入活动及其影响记录了超过 1.64 亿个数据点，这些都为成本和风险预测提供了丰富的基础，也是我们了解当今市场安全与资产保护情况的关键。

通过收集并分析调研数据，我们总结出了许多安全特性信息。这些特性都会影响安全保护环境的显性容量、效率及可靠性。此外我们还评估了安全运营与业务运营的协同情况。我们对它们所表现出的行为进行了规划和建模，形成了可能的部署选项。若要实现这些选项，就需要更高的服务器性能来保证，因为安全运营的最终目的是保护业务流程和运营，而不是掩藏。尽管容量需求和吞吐量会对安全系统造成很大的影响，但需要结合业务的角度来看，因此也更贴合当今的市场情况。业务运营与许多因素有关，包括可靠性、安全程度、人员配备水平、总体安全成本（包括恢复成本）等。这些都与 IT 部门经理、首席技术官、业务领导者的日常决策密切相关。

## 易受攻击拓扑

就安全领域的风险和漏洞而言，其中一个关键因素就是易受攻击拓扑。该拓扑能够量化不同架构之间的相对弱点。

基础性架构不同，对应的易受攻击拓扑也会大相径庭。通过我们对超过 13.1 万家组织的总体分析，我们可以看出这种差异，如下图所示。




最明显的差异在于平台架构、芯片设计、操作系统及堆栈集成方法背后所体现的基础结构和战略。

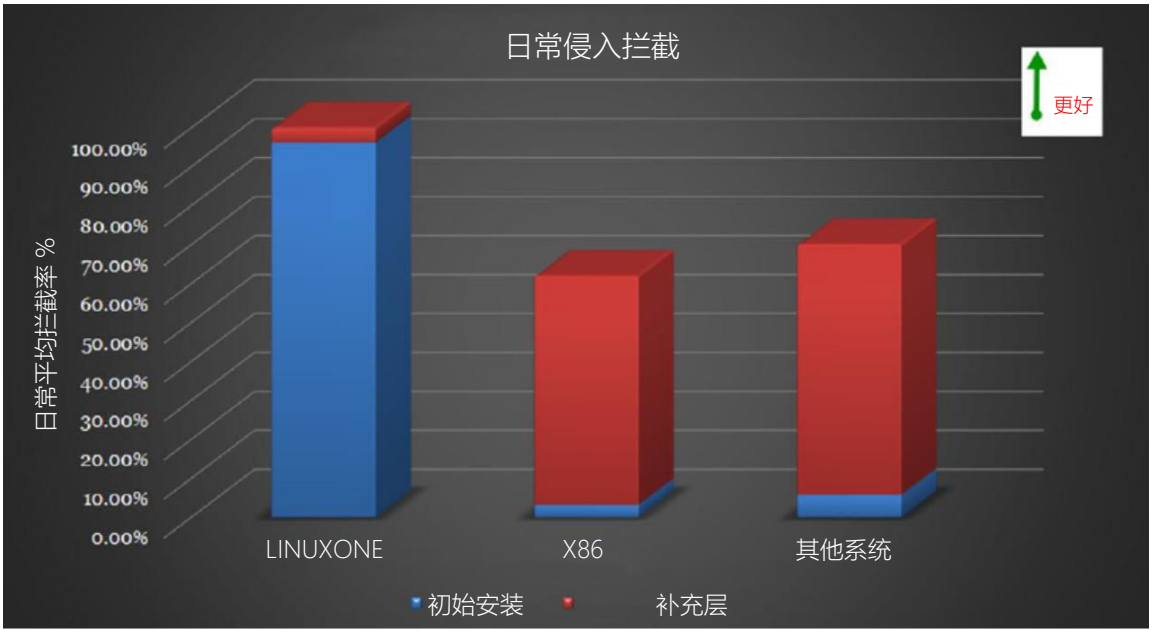
LinuxONE 安全解决方案所采用的安全方法与组合式保护解决方案所用的截然不同。在采用更广泛的安全接口组的情况下，如果在设备级别上来定义安全保护，组织的数据和流程最容易出现漏洞。

更有效的战略是将策略控制与定义汇聚到更集中的一点上。LinuxONE 这种高度集成的内嵌式安全堆栈可帮助组织实现巨大的优势。再加上 LinuxONE 的一流灵活性，便可通过所选的架构充分发挥这款核心平台的优势。

## 侵入弹性

成功安全保护的主要指标是所捕获的、遏制的或制止其造成任何形式损害的侵入数量。该指标所统计的攻击不包括已被插件式防火墙和安全设备拦截的侵入。换言之，只有那些被平台上的安全解决方案拦截的攻击，才会计入到该指标的衡量范围。之后，我们会基于虚拟机的实际数量对统计得出的攻击次数进行标准化计算，因为每个虚拟机都代表着一个单独的逻辑实体。该指标是一个指示性指标，因为我们不会根据每个 VM 中的用户数量进行任何调整。

每个平台的初始安装所提供的侵入拦截水平构成了所需或安装的任何插件式安全组件的基础。下图所示的是初始配置及补充层所提供的安全保护水平，以拦截到的侵入次数百分比来表示。




从初始安装来看，LinuxONE 安全解决方案所提供安全基础的拦截水平最高可以达到其他平台解决方案的 *15.74 倍*。此外，LinuxONE 解决方案可提供比竞争性产品水平高出 96% 的基础性保护，即便没有备用架构的附加性补充亦是如此。

补充性安全层是指插件式应用、策略和技术等。每个组织所采用的此类应用、策略和技术都各不相同，但都是根据自身的安全监管结果、态势及治理水平而确定的。补充性安全需求的水平越高，就意味着需要提高安全软件和人员的投入水平。

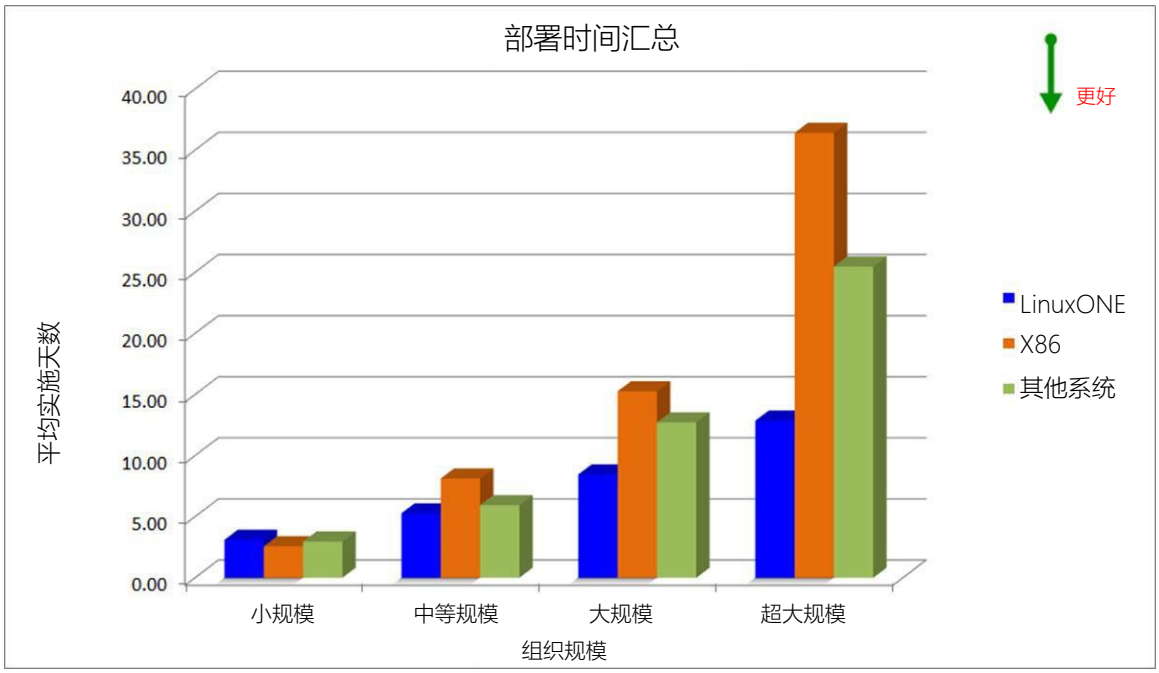
智能资本、自动化服务再加上 LinuxONE 网络安全解决方案的架构设计，就可以大幅提高侵入拦截率。相比其他备选平台解决方案所提供的安全基础再加上其他补充性安全策略、技术和程序所能实现的安全保护水平，LinueONE 平台交付的基础侵入拦截率要高出 *61.4%* 。

若要深入了解安全解决方案的保护效率，还需要进一步进行评估。安全服务首先要以架构为基础，包括各种硬件、软件和中间件组件。在基础之上是各种组织策略、程序、态势与治理。尽管我们可以根据当前的最佳实践对这些加以衡量，而且它们也都属于关键差一点，但我们本次调研的重点在于从硬件、软件、中间件及操作系统的角度来评估供应商的解决方案。

## 敏捷性和灵活性

网络空间的客户都期望响应性。无论优化需求或问题响应背后的原因是出于创新目的还是受市场变化的影响，如果无法实现优化，都会让企业陷入被动境地。

若要了解特定平台的差异所在，我们对组织向 SIL 报告的百万个体验点进行了分析和汇总，结果如下图所示。该图显示了经标准化处理的 200 个功能点应用的平均部署时间。为了避免由于工具不断升级带来混淆，我们考量了在去年实施的分析师部署项目。




组织在基础性架构上部署新版本或新应用时所花费的时间存在着很大差异。LinuxONE 平台中内置的优化能够增强配备、测试及其他因素，提升部署敏捷性，因此该平台所需的部署时间仅为其他平台所需时间的 *35.3%* 。

这种敏捷性的提升非常重要，因为大多数组织每年要部署的升级和发布即便没有数百次，也有数十次之多。从初期安装到部署各个环节的时间节省都有助于直接降低成本并提升客户的响应性。对于网络空间的业务运营而言，该指标已成为最重要的指标之一，因此非常值得关注。

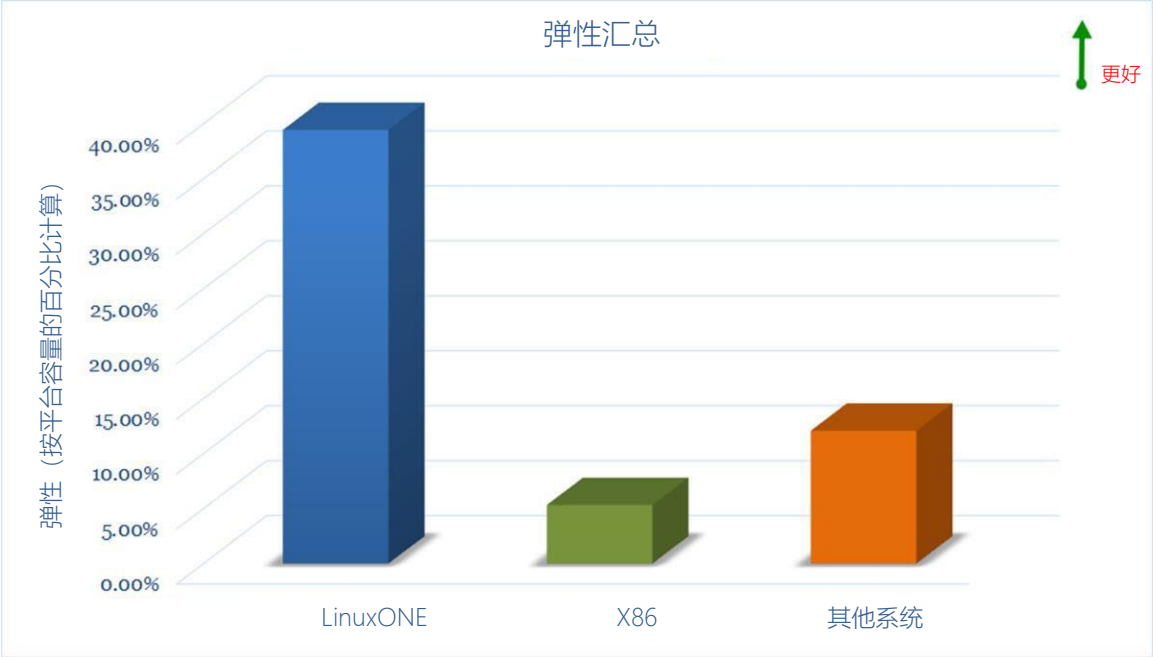
客户对数字空间灵活性的需求可以转化为 IT 和业务部门的贡献。从业务的角度来说，灵活性主要是指战略和方法。具体来说，就是指组织愿意根据市场或客户需求调整运营方向。

除了把控组织运营方向的运营原则之外，业务灵活性还包括对服务和产品的调整，使它们能够始终保持与客户群的相关性。从这一点上来说，这些都与 IT 平台没有直接关联。

从物理与虚拟平台的角度来说，灵活性是指广泛规模的可调整性。随着本地化支持需求的兴起，平台必须要允许高效的再配置。如果由于季节性的原因或市场反响利好导致需求剧增，平台应能够满足这些需求。

关于实施的弹性，可以将其理解为组织在平台不出现整体故障的情况下应对非预期资源需求的能力。极端的例子就是由于集中的服务拒绝攻击导致部署出现瘫痪。部署实施的弹性取决于操作系统和硬件的功能与弹性。在评估所购硬件及所部署的操作系统时，弹性是个典型的考量指标。

下图所示为各个平台的弹性评分情况。弹性评分本身是指在作为此次调研的一部分所进行的生产实施中记录并报告的扩展拐点数量。评分以工作负载百分比的形式表示，表示的是在不对整体运营造成不利影响的前提下，调度算法、缓冲机制及其他组件可容忍的队列构建及应力数量。




LinuxONE 部署的弹性与其他解决方案存在着显著差异。相关报告显示，LinuxONE 实施的平均弹性是其他平台的 *7.41 倍*。这意味着能够减少 IT 解决方案的过度设计，进而可以降低总体拥有成本 (TCO) 和总体信息成本 (TCI)，后者也是经常使用的一个业务指标。

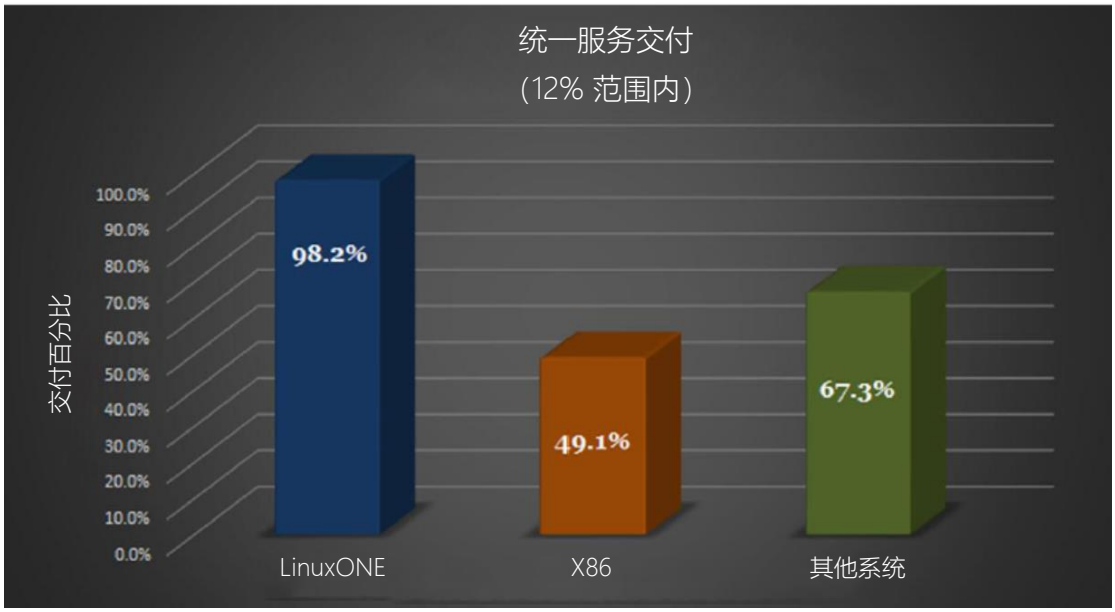
弹性的另一方面是交付统一客户体验的能力。相关数据表明，可预测且统一的客户体验是确保客户满意度的关键。不可靠或多变的客户体验会让买家感到不放心，进而增加支持呼叫及投诉的数量。

统一响应时间的交付主要取决于平台本身。尽管应用设计会针对客户的整体数据流量提供一个框架，但统一性实际上还是由基础架构的内部功能所控制。

我们通过分析针对响应较慢而提出的超过 1,700 万次投诉发现，响应时间变化的识别阈值约为 12%。在此基础上，本次调研对平台的性能进行评估，以了解哪一部分的事务处理响应时间处于该阈值范围内。

值得注意的是，所评估的应用来自于不同的客户、供应商及内部应用。对于该项评估，我们没有进行标准化处理，因为我们要了解的正是不同应用在响应同一活动时的差异。

除了位于阈值范围内的变化百分比之外，在保护行为方面观察到的变化量也会随着架构的不同而有着显著差异。在相同机制的影响下，IBM LinuxONE 同样可以支持统一交付，因此变化量也非常小。




LinuxONE 解决方案的统一交付能力评分是其他平台的 *2 倍*。此外，尽管其他解决方案的响应时间变化量是平均响应间隔的 *17 倍*，但 LinuxONE 最大的记录变化量也才只有 *36.2%*。

通过与不稳定、不统一的数字服务交付进行对比，IBM 的解决方案导致客户对响应时间不满意的几率微乎其微。

# 成本与开支

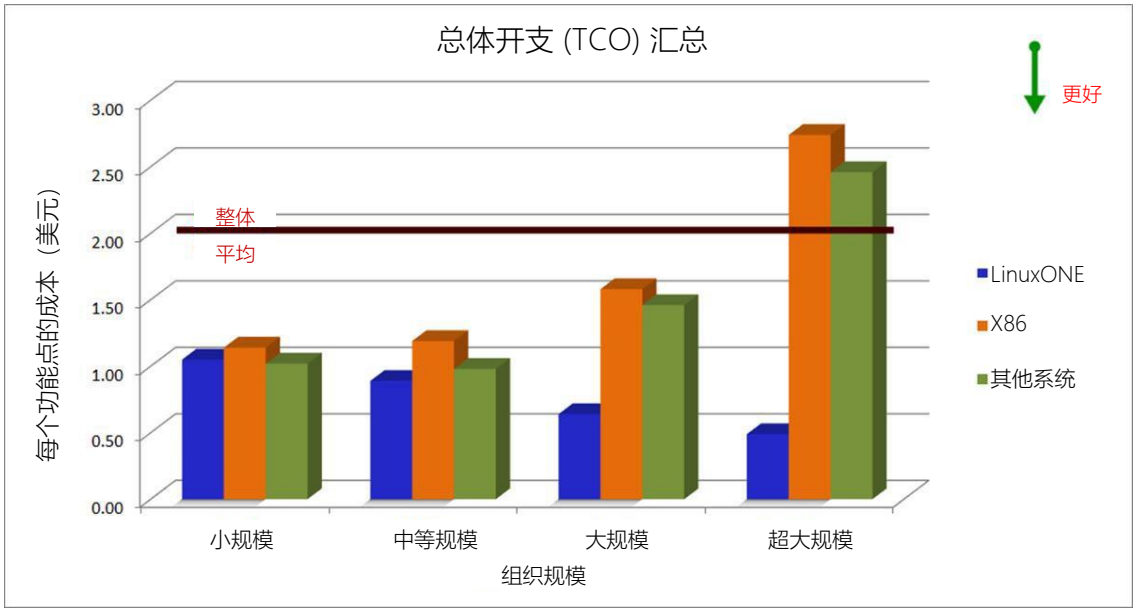
成本是主要的业务考量指标之一。优化收入同时最大程度降低成本，是各个行业都在持续追逐的目标。尽管成本与开支考量的方式有很多种，但多数公司在进行这方面的财务审核时最常使用的指标就是 TCO 和 TCI。由于这两个指标均可通过功能点等标准工作负载单元进行标准化处理，因此无论是小公司还是超大型企业，都适于采用这种对比方法。

在考虑是否在网络空间中开展业务运营时，成本的可控性和局限性都是需要考虑的因素。由于没有像实体店一样的管理开销，因此在数字市场上开展运营可显著提升利润水平。

## 总体拥有成本

TCO 是业务部门衡量运营效率时最常采用的指标之一。该指标可以将整个组织内部各个运营环节的开支汇总到一起来考量。同样地，项目及其开支都会基于相关标准进行标准化处理。如此一来，就可以对大型组织和小型组织进行更为准确的对比。

通过基于功能点等标准工作负载单元对 TCO 进行标准化处理，我们就能够进行准确对比，同时突出其中体现的趋势。从下文的开支对比图可以看出，随着部署项目复杂性的提高，某些类型平台的 TCO 也会呈上升趋势。




但 LinuxONE 的情况却刚好相反。单位开支的下降会转化为规模效率，其中通过利用框架和基础，可形成一个成本高效的财务投资模型。从上图可以看出，LinuxONE 安全实施项目的开支要比其他平台低 81.12%。

这种优势部分是因为 LinuxONE 结合采用了架构化组件与高度可扩展的平台。这种组合的效应也得到了验证，即：架构的负载量越大，工作负载单元所能实现的成本降低就越显著。但凡是在专门针对高度可扩展环境而设计结构的情况下，都会出现这种足迹，但这种足迹往往仅出现在硬件中。在此情况下，无论是物理硬件还是操作系统，都会出现面向可扩展性而进行设计的共性。

> *"Our LinuxONE 虚拟机获得了非常好的投资回报。每个虚拟机的增量成本非常低，而且配备和修改起来速度更快。如此一来，我们就能够降低人员成本，这对我们组织而言是个巨大的挑战。如果我们希望某个系统能够快速扩展，毫无疑问就会将其部署到 LinuxONE 上。总而言之，我们可以更轻松控制成本，也能够更快速、更轻松地完成部署。"*

某家中型制造企业的首席技术官

当系统的复杂性增加时，比如说向上扩展用户时、个人设备（BYOD）数量激增时，或者广泛部署云应用时，架构的可扩展性就会变得尤为重要。云采用的不断增多以及越来越多的应用在云端部署，提升了维持响应性安全、统一响应时间及灵活应用的难度。同时，云部署的形式也进一步加剧了这一挑战的严峻性。无论是私有云、公有云、社区云还是混合云，部署相关的运营与安全实践都必须要进行持续演变。

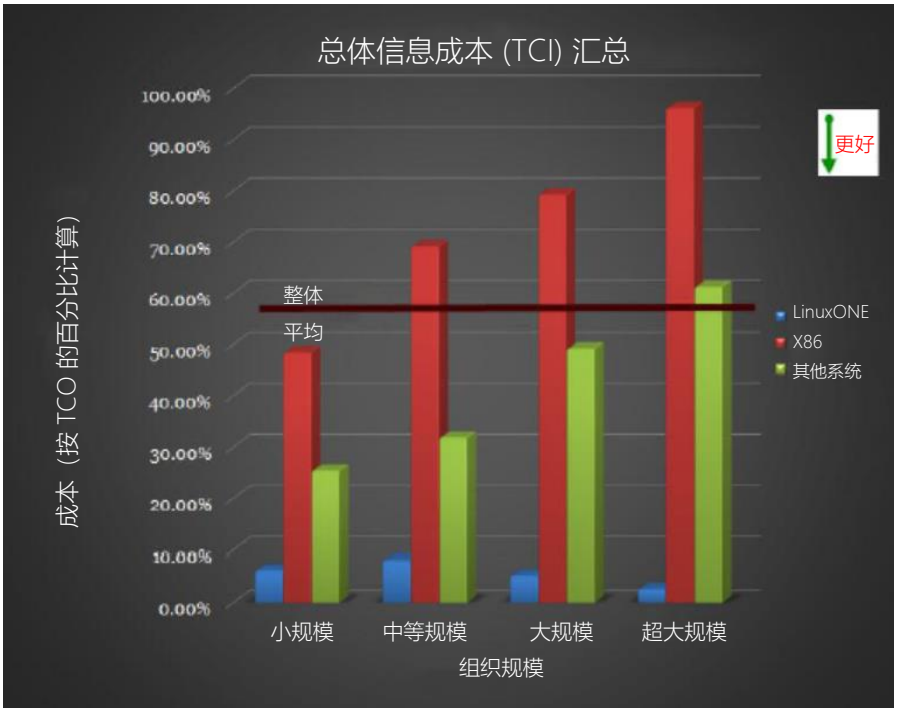
## 总体信息成本

与数字业务相关的成本不仅包括传统的 TCO 指标，还包括一个新兴指标 TCI；通过该指标，我们可以更全面地了解整个组织内部的成本情况。

TCO 是指组织持续运营所必需的开支。该指标涵盖的成本包括：IT 运营人员成本、应用支持成本、补充运营人员或解决问题所需外部服务的成本、电力和冷却开支、硬件和软件维护与许可成本、机房租金等等。

TCI 是指组织维持并保护 IT 资产与知识产权 (IP) 资产所需的开支。这些资产包括数据、业务流程、研究、应用结构及其他知识产权等。该指标所涵盖的成本包括：用于容纳和部署资产的基础架构成本，以及确保资产安全与高效运行的人员成本、电力成本、冷却成本、安全措施成本等。该指标还会考虑 IP 损失和损害的负面影响以及丧失的机会，例如服务拒绝和宕机等。TCI 是最能反映 IT 安全对整个组织的影响的指标，因为它的基础在于对安全的反映式衡量。

在评估不同架构的 TCI 时，我们可以通过多种方式来汇总诸多相对问题。由于基础架构部署的规模存在很大变化，因此基于 IT 与 IP 资产的总价值来进行汇总，从统计学上来说并不明确。因此，我们采用了标准化的对比方法，按 TCO 的百分比来表示 TCI。具体汇总结果如下图所示。



无论是何种规模的组织，IBM LinuxONE 实施的 TCI 成本都非常低，最多可比其他平台低 *92.04%*。由于该指标是新实施成本的一个关键驱动因素，因此这个较小的因素会提升 LinuxONE 部署项目的扩展效率。在进行 TCI 对比时，我们纳入了可用性成本、侵入影响及宕机指标等，确保没有其他额外因素会被纳入到考虑范围。解决方案之间的差异主要体现在三个方面，分别是：

- 人员成本
- 侵入影响造成的成本
- 基础架构的插件成本

人员成本和基础架构成本都是可审计的，而侵入影响造成的成本则需要结合考虑主观因素和客观因素。无论怎样，所有的成本数据都直接来自于客户报告，我们没有对其进行任何改动；不过，我们还是按照调研领域的常规做法对其进行了汇总和平均计算。

无论是从传统开支项的角度来看，还是从侵入造成的反映性开支来看，LinuxONE 安全配置的相关成本都要低于 x86 及其他安全解决方案的成本。这也反映了高度集成式安全堆栈与组合式安全方法之间的差异，而采用后者的话，安全方面的薄弱点和漏洞会不断增多。

## 人员配备

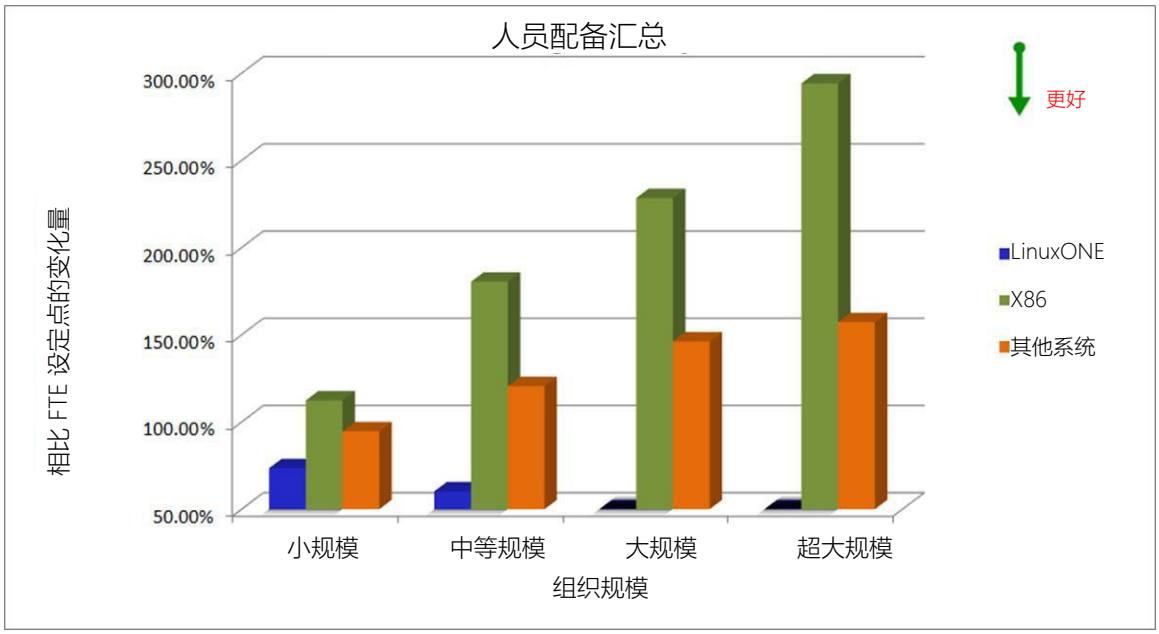
系统管理员与基础架构之间接口的高效性是一个非常独特的基础性因素。该因素涵盖了软件、硬件、操作系统组件及其对人员配备的后续影响。随着人员效率的增加，生产效率水平也会提升；如此一来，完成相同任务所需的投入也会随之减少，这也意味着每个员工的效率会更高。

> *"我们对 LinuxONE 环境非常满意！相比其他 Linux 环境，该平台更稳定，出现的问题也更少。对于同样的工作负载，LinuxONE 只需配备四名全时员工即可，而如果是 x86 平台，则需要配备 13 名全时员工和 2 名兼职员工。现在，我们已经在 LinuxONE 上部署了更多的虚拟机，因为它的设置和配置更快、更轻松。"*
>
> 某家中型制造企业的首席信息官

对于会对用户体验造成影响的任何特定组件而言，它们的效率都很难细分到具体的指标，因为如果对比时的划分过细的话，就会由于这种形式而失去对比的意义。因此我们从 FTE 的角度对人员投入进行整体评估，通过一个广泛的指标来进行平台对比。另一个对比指标"安全方面的整体平均人员投入"也体现了下图之中。该平均指标汇总所有报告中的数据，与组织的规模无关。

我们在对比时采用的人员投入水平是对于每个操作系统组都能维持"黄金标准"环境的投入水平。我们将系统上的工作负载进行了标准化处理，使它们达到同一水平，以维持之前对比中所定义的同一水平对比组。对比设定点为整体响应组的中间值，因为就安全组件而言，可用的选项非常之多。

由于不同架构所用的实施标准集互不相同，因此在评估人员配备情况时，必须将这些标准的严苛性考虑在内。IBM LinuxONE 的部署和使用对安全人员技能水平的要求非常低，其直接原因在于其运营堆栈的集成式性质。当组织规模扩大时，或者组织计划采用云服务交付模式时，这一点尤为重要。

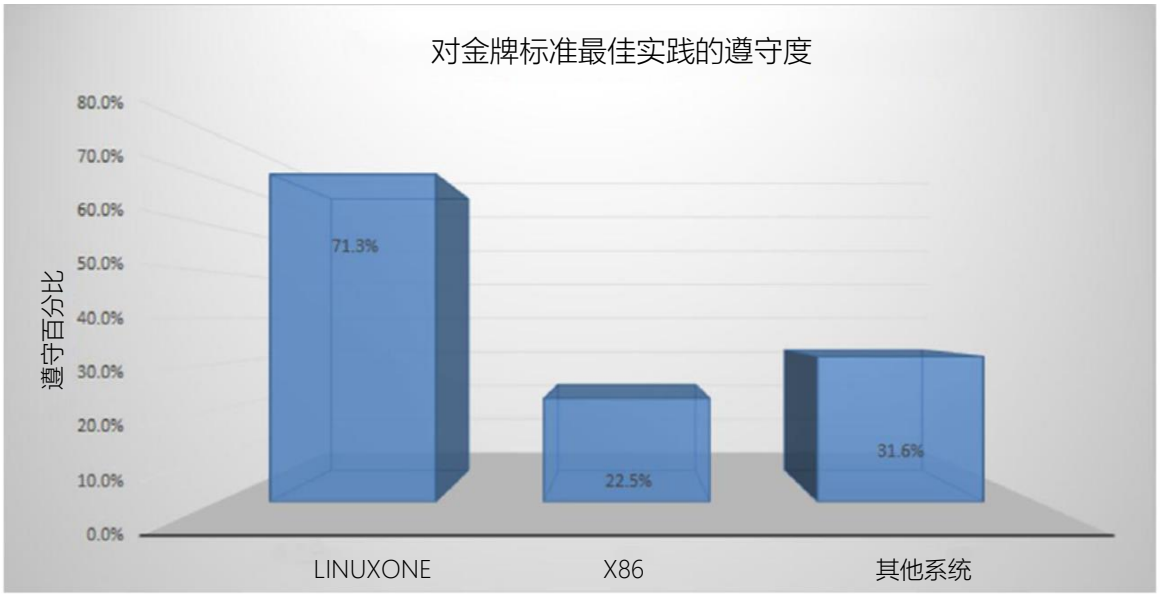



根据详细的客户报告，LinuxONE 部署所需的运营人员工时数比其他平台要少 61.07- 88.05%。

根据运营人员以往的生产行为所体现的效率来看，单个人员的工作量较少。从产业心理学的角度来说，让单个员工在环境切换最少的情况下完成工作是确保效率的关键。这样不仅能够减少由于混淆造成的出错数量，还意味着员工可以将其专业知识运用到以下最佳实践之中。

系统管理、安全、运营等各个领域的最佳实践是限制风险的重要因素之一，因此对组织而言，执行主动评估并完全实施最佳实践所需的时间是一个非常值得考虑的安全因素。关注组织不同人员之间的专业或技能差异其实没有任何意义。不过，如果最佳实践的实施情况不理想的话，就会放大专为特定任务所配备工具的低效性。如此一来，相应的人员就没有时间去完成既定的日常任务，更没有时间去主动采取战略性措施来提前避免问题，而只能被动解决问题。

通过分析受访组织和站点对最佳实践的遵守情况，我们发现不同的架构会对最佳实践的遵守造成不同的影响。工具集的效率、架构和软件堆栈及其他组件的集成度均有助于提升组织对最佳实践的遵守度。




从具体数据来看的话，在部署了 LinuxONE 之后，相关人员遵守全金牌标准最佳实践的可能性是其他解决方案的 *3.1 倍*。如此一来，不仅能够显著降低成本，而且能够对运营活动的其他环节带来可观的积极影响。

## 侵入成本

另一个成本因素是侵入成本，许多组织觉得它仅适于在安全领域的评估中使用。不过，成本始终都属于一个业务问题，因此在评估业务用例时，也应成本加以考虑。该项成本以侵入的代价为中心。

简单来说，侵入是指在未经许可的情况下成功闯入到组织的格局之中。这种闯入的形式有很多，比如盗窃、破坏、封锁等等。因此，当今的保护机制必须覆盖比确保整个平台级别的安全所必需的更广泛的访问点。在此情况下，处理流程中所有方面的控制都必须到位。许多政府和安全机构都需要确保主要 IT 设施的分配与处理的安全性，包括：I/O、网络访问、内存管理与整体常规执行访问等。

在某些安全侵入情境中，组织需要耗费很长的时间才能评估出成本。专有研究成果被盗就是这种滞后性影响的示例之一。专有知识产权发生丢失可能会产生非常严重的市场影响。

与侵入相关的平均成本代表的是不同技术的相对风险。不幸的是，市场中已经形成了一种"可接受损失"的风气，因为许多小型侵入事件的平均成本并不高。这种情况导致整个市场放松了安全的定义与控制，忽略了更大规模、更严重的侵入事件会带来的非常真实的风险。当某个组织习惯于接受重复出现的"可轻松处理的"损失时，就会导致他们的信息和运营处于易受攻击的状态，随时可能会造成重大损害。

通过评估每次成功侵入事件的平均成本，我们可以了解不同架构可能造成的重大财务影响。下图所汇总的数据不包括由于密码被盗而造成的安全违反事件。


侵入事件的平均成本日益增加，而且增加的速度也在不断加快。相比十年前，侵入事件的相关成本提高了650%。造成这种情况的部分原因在于云应用的范围不断扩展，一旦出现侵入事件，就会有更多的人员和数据受到影响。另一个需要考虑的因素是侵入事件的攻击性越来越强大。这意味着组织在选择 IT 组件时应考虑的威胁水平也越来越高。

侵入事件的平均成本与许多因素有关。侵入检测的速度和效率、隔离侵入以免其造成进一步损害的能力、补救方案的彻底性，都会影响侵入事件的成本。部署 LinuxONE 平台之所以能够显著降低单次侵入事件的成本，就是这些因素综合作用的结果。

## 风险成本

随着网络犯罪对业务造成的损害不断升级，催生了专业化的网络安全保险公司。这一新兴市场正在快速发展壮大，该领域的公司会捕获足够的数据，以便准确地评估客户的风险水平。

参保的组织除了需要部署各种所需的协议和组件之外，大多数网络安全保险公司还会要求他们的客户提供充足的备用金，以供组织在遭受成功侵入后进行合理响应时使用。

值得注意的是，由于 LinuxONE 系统遭受安全侵入的可能性非常低，因此这些系统所需的备用金仅为其他平台或解决方案的 3.2%。行业内的平均备用金水平是 14.7%；从这一点来说，部署 LinuxONE 可为组织带来显著的业务优势。

对于在网络空间中开展业务运营且需要计算风险的组织而言，这一数据就为他们提供了一个清晰、简明的跨行业视角来考虑财务风险和预估成本。这种备用金的影响仅仅是"冰山一角"。

面临着这些备用金需求的高管们已经开始如何更多地从总体拥有成本的角度来考虑成本，而不是仅仅关注于采购成本，正如一位首席执行官在近期的一封电子邮件中所写的那样，“采购成本是一次性开支，而备用金则是持续开支。如果要我在运营预算中长期为单个系统准备 750 万美元的备用金，我是说什么也不会干的。”

这一点非常值得高管们深思，而且在选择或部署平台所需的业务用例评估时，也应对其加以考虑。

# 结论

*华盛顿的一家联邦上诉法院做出规定，如果企业未能履行保护客户个人数据的义务，消费者可以提起诉讼。在此案件中，EPIC 提供了一个“法庭之友书状”，其中申辩说“如果公司未能采取合理的安全措施，消费者将会继续面临遭受数据泄露的风险。”上诉法院同意 EPIC 的观点，认为低等法院驳回该案件的做法是错误的。*

美国电子隐私信息中心，华盛顿巡回上诉法院维护数据泄露事件受害者寻求法律救济的权利，2017 年 8 月 1 日

相比市场上的其他平台，当前版本的 LinuxONE 平台在 TCO、性能和风险等方面具有显著的优势。当前可用的选择性加密级别以及原生平台对抗常见威胁向量的能力，都可以为组织提供坚实的安全保护基础。

对于在网络空间积极开展业务的企业和已迁移到云模式的企业而言，它们都对网络安全非常敏感。组织所拥有数据及其他智能资本的安全正在快速成为一个主要关注点，因为我们所处世界的互联性正在日益提升。伴随着集成度的提升，随之而来的是各种巨大的挑战，因为组织需要经历保护他们的市场优势和财务收益。IBM 在资产保护与高度安全部署领域拥有丰富的经验，而 LinuxONE 解决方案可提供其他解决方案所不具备的丰富功能。

下表汇总了本次调研的一些重要结果。

*快速汇总表*

| 类别 | 注释 | 要点 |
|---|---|---|
| 上市时间 | 通过 LinuxONE 平台让系统上线运行所需的时间仅为通过其他平台所需时间的 *35.3%*。 | 让系统更快地上线运行。 |
| 灵活性 | 相关报告显示，LinuxONE 实施的平均弹性是其他平台的 *7.41 倍*。 | 更轻松地解决非预期的活动高峰。 |
| 灵活性 | 运行 LinuxONE 平台的客户最高可实现的最终用户请求交付统一性是使用其他平台的客户的 *2 倍*。 | 通过统一交付改善客户体验。 |
| 总体拥有成本 | LinuxONE 安全项目的实施开支最高可比其他平台低 *82.12%*。 | 相比竞争对手的产品，可显著降低 TCO。 |

| 类别 | 注释 | 要点 |
| --- | --- | --- |
| 总体信息成本 | 无论是何种规模的组织，IBM LinuxONE 实施的 TCI 成本都非常低，最多可比其他平台低 *92.04%*。 | 显著降低信息相关成本。 |
| 人员 | 运行 LinuxONE 系统所需的 FTE 数量只有其他系统所需数量的 *61.07-88.05%*。 | 用更少的人员完成更多的任务。 |
| 风险和成本 | 网络保险公司实施 LinuxONE 所需的备用资金仅为实施其他平台的 *3.2%*。 | 减少所需的备用资金。 |
| 风险 | SIL 风险分析团队通过分析得出 LinuxONE 平台的风险级别仅为其他解决方案的 *1/20*。 | 显著降低安全风险。 |
| 安全效率 | 从初始安装来看，LinuxONE 安全解决方案所提供安全基础的拦截水平最高可以达到其他平台解决方案的 *74 倍*。 | 通过集成式的安全方法实现最安全的应用环境。 |
| 安全效率 | 就部署 1,000 个应用的实施项目而言，LinuxONE 实施项目的成功安全侵入次数*不到其他平台的 0.01%* 。 | 部署相比竞争对手更高效的基础性安全平台。 |
| 人员 | 在部署了 LinuxONE 之后，相关人员遵守全金牌标准最佳实践的可能性是其他解决方案的 *3.1 倍*。 | 节省时间和资源，用于推动创新。 |

数字业务固有的多变性正在不断加剧。变化速度更快、攻击形势更为严峻，而风险管理角色面临的挑战也日益增多，这些不仅带来了机会，也意味着巨大的风险。

在 SIL 进行的此次调研中，其最初目的是从平台架构的角度来分析业务安全对真实世界的影响。为此目的，我们对 x86、IBM LinuxONE 平台及其他产品进行了对比。

通过对比分析我们发现，就整个行业而言，企业在选择计算机架构时的考虑事项正在发生着巨大的变化。

## SOLITAIRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL) 是一家致力于实用的预测性能建模的专业级服务提供商。SIL 成立于 1978 年，主要利用广泛的 AI 技术和专有混沌数学来分析预测场景或取证场景。SIL 的分析服务已经为超过 7,600 家客户提供了持续风险分析、性能根本原因分析、环境影响、容量管理、市场趋势、缺陷分析、应用 Fourdham 效率分析、组织动态杠杆识别及成本与开支分析。SIL 还可针对供应商对全球各地政府组织及许多商业公司的响应提供 RFP 认证服务。

目前，已有大量商用及政府用硬件与软件提供商与 SIL 展开了合作，旨在获得产品性能和局限性方面的认证。SIL 也与这些供应商建立了合作关系，旨在改善客户部署项目的吞吐量和可扩展性，同时为其提供风险概要及其他风险减缓战略。最近几十年来，SIL 积极参与行业标准的制定及性能认证，而且一直都在针对运营特性化主题研究 (OPMS) 收集信息，该研究的目的是更好地了解以 IT 为中心的组织成本和行为特性。OPMS 的研究成果会不断丰富 SIL 的启发式数据库，其信息规模目前已超过了 538 PB。随着基础统计数据的不断丰富，也将会不断改善 SIL 分析服务的准确性和效率，将其提升到业内独一无二的高度。总体而言，SIL 每年都会运行超过 16 个模型，以满足持续订阅客户和临时查询的分析需求。

## 调研方法说明

为了了解 LinuxONE 平台作为组织 IT 基础架构的一个关键部分而带来的影响及其对客户体验的影响，我们评估了大量的部署项目。我们从多个因素（如宕机总次数）入手对比了不同平台在运行行为上的差异，以了解各自功能组合的实际效果。衡量这些实际效果的指标包括总体性能、容量使用情况及其他重要业务指标。

SIL 所用的方法是基于真实的系统和业务活动，对运营生产行为进行汇编和关联。在本次调研中，我们一共观察、记录并分析了 13,041,692 个环境设置来证明我们的调研结果。此外，我们还收集了与部署数据相匹配的客户体验数据。我们一共分析了超过 810 万份客户反馈的体验报告，将其与 IT 环境进行了匹配，而且也纳入到了此次调研之中。借助广泛的客户与行业体验数据，我们能够更准确地了解真实运行环境中的行为。借助来自这些系统的数据，我们得出了与组织当前运营挑战和收益相关的信息。此外，我们还对客户报告的系统行为进行了分析，得出了有关不同架构的原始性能和实际业务影响的特性数据。

作为此次调研内容的一部分，我们评估了新兴技术对不同组织的整体性能、成本和风险的影响，因此使用客户提供的额数据进行了详细的运营模拟。我们使用参与模拟的组织所提供的数据模拟了这些组织的虚拟环境，并在其中运行了为期 14 个月的日常活动。模拟的结果包含在本白皮书的调研结果部分。

在此次调研中，我们使用相应的分析方法将运营数据纳入到分析范围内，其中包含了非常详细的系统活动信息。值得注意的是，运行这些生产平台的客户为我们提供了所有此类信息。另外需要注意的是，在此次调研中，我们没有收集来自人工基准或构造测试的数据，因为此次调研的目的在于了解整个组织内部的实际运营过程，而不是他们对当前所部署系统的感受。因此，这些分析结果代表的是真实的运营情况，而不是人工基准配置情况。由于此次调研的重点并非找出操作系统或硬件的各种细微差异，因此我们对这些操作系统或硬件的所有发行版进行了汇总，旨在找出它们之间的整体架构差异。通过这种方式，我们可以从更广泛的角度来了解他们的架构战略。

为了确保此次调研的结果更具代表性，我们收集了来自许多不同部署项目、行业、地域及供应商的信息。在所收集的信息中，会存在一些数据重叠，因为单个组织可能会同时选择多个供应商的产品。在这些情况下，某些组织的百分比总数可能会超过 100%。

对于采用多层部署（例如涉及到多个地域位置或行业分类）的组织，我们按照所有指标对他们的反馈数据进行了筛选。我们进行了额外筛选，目的在于将不满足最佳实践的实施项目排除在外。由于许多此类实施项目中的高故障率、低性能和高成本等特点几乎与实际的硬件和软件选择无任何关系，因此这些项目已被我们排除在了此次调研的分析范围之外。

此次调研涵盖的行业包括制造业（24.17%）、分销行业（11.38%）、医疗保健业（7.56%）、零售业（14.00%）、金融业(21.91%)、公共领域 (7.61%)、通信业 (11.47%) 及其他行业组 (1.89%)。

受访组织的地域分布如下：北美地区 41.38%；中美洲和南美洲 10.61%；欧洲 23.68%；环太平洋地区及亚洲 21.23%；非洲 3.04%；其他地区 0.07%。

由于不同规模组织的平台部署战略和收益差异很大，因此 SIL 按小型、中型、大型和超大型规模进一步对组织进行分类。在进行分类时考虑了组织的员工数量及年总收入。员工数量乘以年总收入就构成了整个分析中所用的一个指标定义。在该定义中，小型组织是指员工数量少于 100 人、年总收入低于 2,000 万美元的组织，或者指标值为 2,000（员工数量 100 X 年总收入百分美元数 20）的组织。员工数量为 50、年总收入为 4,000 万美元的组织在分析时也归类为小型组织。SIL 在分类时所用的指标值阈值分别为 2,000（小型组织）、10,000（中型组织）、100,000（大型组织）和 1,000,000（超大型组织）。

本次调研中的信息也会被收集，这也是 SIL 自 1978 年以来一直执行的持续数据收集与系统支持实践的一部分。所有测试均由客户人员在 SIL 的客户场所执行。测试结果通过安全的常规数据收集点送往 SIL；自从与 SIL 建立支持关系之后，客户一直都是使用这些数据收集点发送数据。由于信息是通过安全的数据点收集而来，因此，标准的 SIL AI 处理系统会采用标准格式处理数据，并从中去除了所有的详细客户信息。之后，这些经过滤的数据会输入到系统供分析之用。

## 归因和免责声明



本文档的编写获得了 IBM 的资金支持。尽管本文档可能会使用包括 IBM 在内各种不同供应商的公开资料，但就本文所述的各个问题而言，本文并不代表此类供应商的观点。

ZSL03452-CNZH-00