对标洞察

IBM 商业价值研究院

零信任安全性入门

建立网络弹性之指南

中国洞察

IBM

IBM 如何提供帮助

IBM Security 使用与业务优先任务保持一致的现代开放式安全方法，将零信任付诸实践。要了解更多信息，请访问：ibm.com/security/zero-trust

为了更好地了解组织如何实施零信任安全性，IBM 商业价值研究院 (IBV) 与牛津经济研究院合作，对来自全球 15 个行业的组织中的 1000 多位运营和安全高管进行调研（请参阅第 16 页的“调研方法”）。

扫码关注 IBM 商业价值研究院

了解更多 IBM 零信任安全解决方案的详细信息，请扫描二维码。或者致电 4006657755，与专家取得联系。

官网

微博

微信公众号

微信小程序

零信任安全解决方案

冯靓、高爽、张炜、王莉、Chris McCurdy、Shue-Jane Thompson、Lisa Fisher 与 Gerald Parham 合著

要点

新业务模式正在加快安全转型的步伐。
随着风险的持续演变以及新威胁的不断出现，依靠既定边界和绝对信任的传统安全模式逐渐过时。超越传统职能和组织边界的组织需要更为全面、多层次的事件驱动型安全模式。

零信任安全性带来明显的运营优势。
“零信任”是一种动态的安全方法，结合使用访问控制、身份管理和背景数据来验证请求。“零信任率先尝新者”是指那些具备最成熟的零信任能力的组织，他们通过这种方法减少支出，改进网络安全有效性，并提高网络资源保留率。

零信任领先者在 4 个核心能力方面出类拔萃。
零信任安全性通过将信任转化为访问操作变量来增强网络弹性。成熟的 4 项核心能力与相关实践可以推动零信任取得成功。

进步的代价

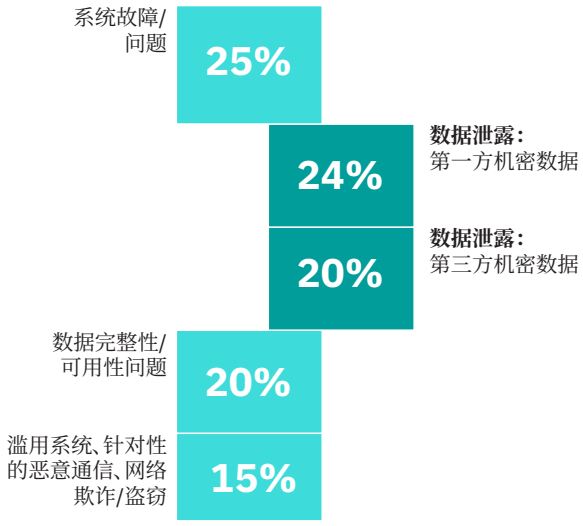
组织通过加快数字化业务转型步伐，扩展云技术的应用范围，扩大远程员工队伍以及整合供应链，以应对新冠病毒疫情的冲击。我们的调研表明，从 2019 年底到 2020 年末，受安全保障的远程工作人员数量增加了 41%。

但是，将交流沟通、业务和个人互动移至线上也显著扩大了潜在的攻击面，导致网络安全事件和泄露的记录大幅增加（见图 1）[1]。随着工作负载迁移到云端，威胁也如影随形。我们的调研表明，在 2020 年，超过 90% 的网络相关事件起源于云环境。

图 1

数据暴露

在线互动越来越普遍，中国的数据泄露也越来越常见*



问题：贵组织检测到的网络安全事件按类型是如何分布的？
** 由于对数据进行了四舍五入，总和可能不等于100%*

76%

的中国企业无法保护在多个云和本地环境中移动的数据，严重阻碍了价值实现。

87%

的中国企业无法安全地为内部和外部合作伙伴实现和扩展新的云原生能力。

150 天 —

中国企业用合格的候选者填补网络人才空缺所需的时间，导致意识和责任产生缺口，增加风险敞口。

虽然基于云的共享服务和协作式工作环境对于实现业务成果至关重要，但这些环境需要一种新的安全运营方法 — 一种更加灵活、响应更迅速、合作程度更高的方法。为了利用这种新方法的优势，领先者根据零信任原则对其 IT 和 OT 运营进行现代化改造（请参阅“观点：什么让零信任安全性与众不同？”）。

高价值但易受攻击：保护关键基础架构

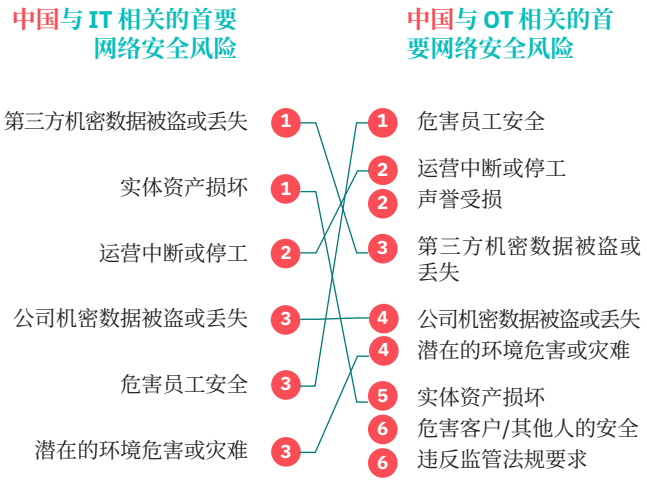
关键基础架构体现出信任与风险之间的动态关系。随着运营转移到线上，IT 和 OT 网络都面临网络攻击风险。我们对 IT 和 OT 环境的依赖意味着任务关键型基础架构在新威胁面前越来越脆弱（见图 2）。

IBM Security 与 Ponemon Institute 合作发布的《2021 数据泄露成本报告》显示，远程工作导致数据泄露成本增加了 107 万美元。[2] 另一份 IBM Security 发布的《X-Force 威胁情报指数 2021》也发现，勒索软件攻击已经成为第一大威胁类型，在 X-Force 2020 年所响应的安全事件中的占比为 23%。[3]

图 2

相互关联的风险

IT 和 OT 风险非常复杂，而且相互关联



问题：您如何对上述网络安全风险评分？该图显示了回答高风险和极高风险的数量（部分选项样本量较少）。

传统的网络安全方法依赖于许可权限和离散的网络边界，但目前的网络由动态服务和扩散的边界所定义。

信任是协作与合作关系的基础。随着这些能力成为价值实现过程中不可或缺的要素，我们对信任的看法也在迅速发生变化。虽然传统的网络安全方法依赖于许可权限和离散的网络边界，但目前的网络由动态服务和扩散的边界所定义。当今的数字平台依靠多方互联互通和共享信息来产生价值。

因此矛盾不可避免。许多 OT 系统传统上依赖于系统隔离，但由于需要使用来自互联设备和智能系统的洞察，使得这种做法难以维持。如果听之任之，缺乏连通性会使现有漏洞更难以修复。

更糟糕的是，风险会不断叠加：一个系统出现故障通常会引起连锁反应。威胁实施者在利用 IT 和 OT 安全控制缺陷方面越来越老到（请参阅“观点：IT 与 OT 系统的融合增加风险敞口”）[4]。虽然潜在影响非常明显，但可能难以预测此类风险。

网络犯罪即服务是令人不安的新趋势。[5] 这些服务通过黑客论坛、直接网络渠道和使用加密货币在暗网上销售，依靠通常是协作式的复杂网络犯罪攻击，例如僵尸网络、分布式拒绝服务攻击 (DDoS)、信用卡欺诈、恶意软件、垃圾邮件和网络钓鱼攻击。

《中华人民共和国个人信息保护法》于 2021 年 11 月 1 日生效，结合先前已经生效的《网络安全法》和《数据安全法》等相关法律法规，形成了我国数据合规的三法联动体系。在我国数据监管越来越严格的背景之下，采用零信任架构，可以有效增强企业的合规优势。[7]

观点：什么让零信任安全性与众不同？

从原理上而言，零信任是一种预防性安全方法，它假定恶意行为者已经渗透到组织的网络防御中。目前普遍认为，IT 和网络安全运营在职能上是相互依赖的。因此，组织感知、评估和响应事件的能力表现出较高的动态性，通常接近实时。这种覆盖 IT 和网络运营的整体意识使零信任能力真正具有变革性。

在实践中，零信任要求对每次价值交换进行认证和验证，从而将各个运营和网络安全领域衔接起来。由于零信任运营模式不依赖于安全边界，因此非常适合组织边界分散并且以服务形式交换价值的共享生态系统。通过将信任作为运营和交易变量，第三方甚至可以支持最敏感的工作负载和任务关键型能力。

观点：IT 和 OT 系统的融合增加风险敞口

中国高管面临的主要 IT 问题是第三方机密数据被盗或丢失、实体资产损坏，以及运营中断或停工。主要的 OT 问题包括危害员工安全、运营中断或停工、声誉受损，以及第三方机密数据被盗或丢失。

虽然与 IT 和 OT 环境相关的网络安全风险并不总是相同，但它们通常会相互加强。正如 Colonial Pipeline 黑客攻击事件中所展现的那样，某个领域的故障可能会导致连锁反应，例如 IT 系统的密码泄露引起 OT 平台的可用性和可靠性降低。[6]

获得零信任优势

我们的分析表明，23% 的组织领先于同行，在 IT 和 OT 环境以及与生态系统合作伙伴的互动中部署零信任能力，我们将其称为“零信任率先尝新者”。

这些组织将其 IT 和安全运营视为一个整体。他们擅长开展内外部合作，以管控网络安全风险。他们对与相互依赖的治理、风险与合规框架相关的安全运营进行现代化改造。他们充分应用云计算、AI 驱动的分析和自动化技术。他们招聘、培养和留住高技能的网络安全人才，以支持在数字资产中实现零信任能力。

最重要的是，他们的安全运营可以适应当前业务环境的复杂性——无论是支持远程员工；监控终端、应用、数据和网络流量；还是分析员工、客户及合作伙伴的行为以发现新出现的威胁。

什么让零信任率先尝新者与众不同？

零信任率先尝新者告诉我们，他们对 IT 预算和资源的投资比例与同行对网络安全的投入比例相似，但他们从安全方法中获得了显著的业务和安全收益。

事实上，在表示显著减少了安全资本和运营支出，同时提高了网络安全能力的有效性的受访者中，率先尝新者的比例是其他企业的两倍之多。具体来说，他们：

- 提高了检测和响应能力，显著减少了敏感数据的泄露。在发生数据泄露事件时，他们能够有效限制恶意软件传播，从而减轻对组织的影响。
- 优先考虑在生态系统合作伙伴之间建立和维持安全连接，从而更有效地利用云投资。
- 将更多的网络安全预算投资于对资源进行技能重塑。因此，他们的网络资源保留率比其他组织高出 10%。

零信任率先尝新者的成功有力说明了全方位零信任战略的优势。这些组织处于有利地位，实现了更高的运营效率和更出色的业务成果。其他组织可以先了解哪些运营能力对于零信任成功至关重要，然后应用这些能力以实现类似的成果。

零信任率先尝新者用于网络安全的 IT 预算比例与同行相似，但收益明显高很多。

立即行动：绘制零信任路线图

零信任率先尝新者在实施 4 项核心能力方面的进度几乎是其他企业的两倍：

1. 零信任安全运营的坚实基础，以治理、风险与合规控制为指导，并由 AI 驱动的分析进行增强。
2. 安全指挥与自动化管理能力，扩大混合云运营环境中安全运营的范围和规模，提高可视性和效率。
3. 零信任安全控制框架，用于监控、管理和保护关键资源 — 包括用户、数据、网络、设备和工作负载。
4. 具有强大适应能力的网络人才管理系统，优先将人才与技术相结合，实现更理想的安全成果。

这些构成要素中的每一个都是通过一系列相互加强的实践和活动所建立的。特别重要的一点，我们的数据分析强调了这些实践和活动相互依赖的程度。换言之，所有 4 项核心能力共同发挥作用，实现零信任带来的优势（见图 3）。

图 3

在设计中就考虑安全

零信任能力相辅相成

来源：IBM 商业价值研究院数据分析。

加强风险意识和恶意软件传播控制力度可显著降低网络攻击的风险。

由于每个组织的 IT 和网络资产反映各自不同的需求，因此他们的零信任之旅都具有独特性。影响组织零信任之旅的因素包括业务战略和运营模式；预算和资源可用性；合作关系的广度和深度；现有技术的实施和限制；特定于行业和地理区域的监管要求和竞争要求。

考略到这些因素的多样性，我们的方法优先考虑实用性、灵活性和基于现有能力的优点。我们提供的建议都源自运营绩效洞察，基于各种运营环境的现实成果，包括专注于增长的年轻组织，以及专注于转型的成熟组织。

对于每个构成要素，我们提供说明、与之相关的优点以及实现要素的实践和活动。

构成要素 1：为零信任安全运营建立坚实基础

零信任率先尝新者将零信任能力整合到主要的安全架构和运营之中。这些能力旨在增强现有的技术、流程和技能，而不是取代它们。

这些组织已经建立了基于现代安全实践和自动化安全控制的安全意识文化。这种企业文化通过制定策略，定义可以访问公共网络、应用和数据资产的人员和内容，来提高安全风险意识。

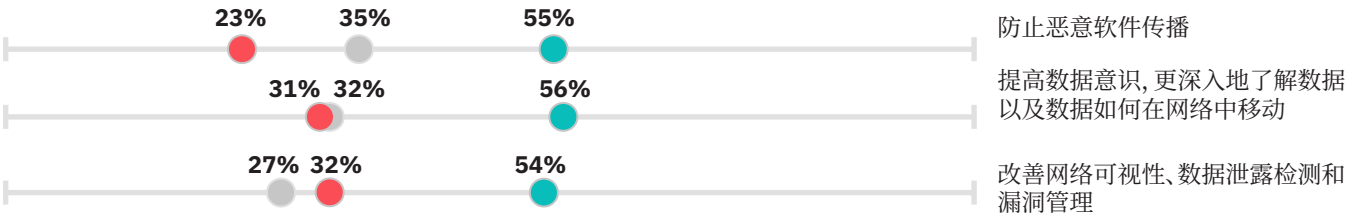
作为补充，还采用技术安全解决方案，系统性地实施这些策略。这种环境有助于确定易受攻击的设备、应用、服务和行为，然后使用自动化控制来帮助消除威胁和漏洞。

当发生数据泄露时，率先尝新者能够阻止恶意软件的传播，这有助于控制风险，降低发生后续问题的可能性（见图 4）。总的来说，加强风险意识和恶意软件传播控制力度可显著降低网络攻击的风险。

图 4

发现并理解

改善网络可视性，实现更理想的结果



** 全球其它企业指的是，除零信任率先尝新者以外的全球其它企业*

问题：贵组织在多大程度上通过安全方法实现了上述每项收益？百分比反映选择显著实现或非常大程度实现的受访者（部分选项样本量较少）。

此外，零信任率先尝新者与合作伙伴携手简化网络风险的管理和报告。在治理、风险与合规框架的指导下，他们在整个企业内以及向战略合作伙伴和第三方供应商主动说明新的威胁。他们使用标准系统开发生命周期 (SDLC) 和 DevSecOps 方法，使安全运营和治理的关键能力实现标准化，进一步提高效率。

通过在事件检测和响应方面广泛应用高级网络安全分析，零信任率先尝新者能够监控更高比例的网络通信 (55%) 和终端设备 (68%)，以发现漏洞和策略违规情况，相比之下，其他同行的这个比例分别为 45% 和 60%，而中国的比例也仅为 50% 和 61%。组织监控的网络通信流量和终端设备越多，发现和修复潜在威胁的能力就越高。可视性越高，成功的可能性就越大。

大多数率先尝新者表示，他们对数据如何在网络中移动有了更为深入的了解。在表示自己提高了网络可视性、数据泄露检测能力和漏洞管理能力的受访者中，率先尝新者的数量是中国的 1.7 倍（见图 4）。

构成要素 1

为零信任安全运营建立坚实基础

监控网络通信中的可疑活动

45% 所有其他企业

55% 零信任率先尝新者

监控终端设备是否存在漏洞和策略违规

60% 所有其他企业

68% 零信任率先尝新者

怎么做

与组织内部和更广泛生态系统中的合作伙伴共同使用 IT 治理和控制

使用 AI 驱动的分析，标记异常情况并触发自动化控制

自动化的 AI 安全模式可识别异常行为，评估漏洞并标记新威胁。

1

尤其值得注意的是，有 2 项率先尝新者实践可帮助组织为零信任安全运营建立坚实的基础：

1. 与组织内部和更广泛的生态系统中的合作伙伴一起使用 IT 治理和控制机制，以提高网络风险规避工作的可视性和有效性：

- 为员工提供安全教育和风险意识培训 — 建立保护组织所需的知识、技能和能力。
- 应用治理、风险管理与合规框架和项目，发现、评估和消除网络风险。根据业务目标与合规要求，平衡可接受的风险水平。与生态系统合作伙伴合作，实现更有成效的规模经济。
- 实施数据丢失防护 (DLP) 策略。定义贵组织如何共享和保护数据，指导工具的实施过程，防止用户向核心网络外发送敏感或关键的信息。与使用共享基础架构的合作伙伴共同开展这些工作。
- 将安全性整合到软件开发过程中。DevSecOps 等云原生方法使组织能够更有效地与合作伙伴合作，特别是通过采用常见的安全运营和治理方法。[8]

2. 使用 AI 驱动的分析，标记异常、触发补救控制措施并防止威胁实施者使用自动扫描和攻击方法：

- 实施高级网络安全遥测能力，包括监控与分析技术，以检测和消除安全事件。对高价值的数据、资产、网段和云服务使用 AI 驱动的自动化调查流程，减少对人工威胁检测工作的依赖。

  可以根据攻击特征和攻陷指标 (IOC) 对威胁进行分类并确定其优先级，然后触发相应级别的警报。为了提高运营效率，组织可能希望通过终端检测与响应 (EDR) 以及跨层检测与响应 (XDR) 能力，补充现有的遥测解决方案。
- 应用 AI 以自动构建模型、跟踪正常行为以及标记异常活动。自动化 AI 安全模型可识别正常（而非异常）行为，动态评估漏洞，并标记可能表示新威胁的异常活动。模型可使用这些输入，定性和量化潜在的风险敞口。

构成要素 2

借助安全指挥与自动化管理能力，强化运营

安全资本和运营成本显著降低

61%
零信任率先尝新者

合规计划的范围明显缩小，成本大幅降低

50%
零信任率先尝新者

怎么做

- **建立生态系统范围的安全运营中心 (SOC)**
- **实施云环境无关的一站式平台，获得覆盖所有提供商的可视性**
- **应用基于 AI 的安全智能，检测异常行为**

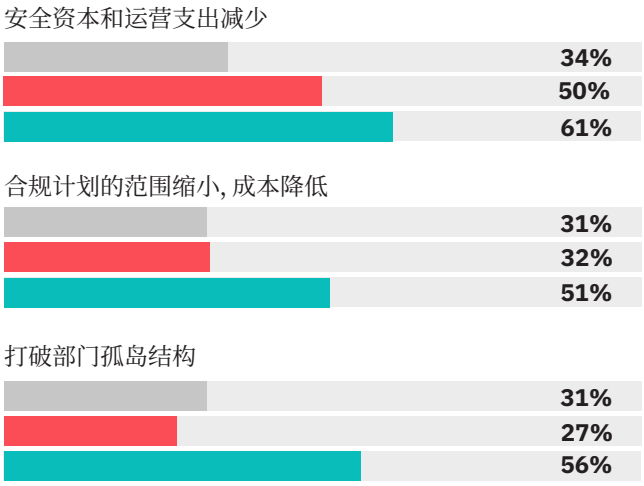
构成要素 2：借助安全指挥与自动化管理能力，强化运营

零信任率先尝新者采用安全指挥与自动化管理能力，扩大安全运营的范围和规模，提高效率。61% 的零信任率先尝新者表明，这帮助他们显著节省了安全资本和运营成本，其中半数受访者表示，合规性计划的范围明显缩小，成本也显著降低。

图 5

成本优势

指挥与自动化管理有助于扩大范围和规模并提高效率



全球其他企业
中国企业
零信任率先尝新者

问题：贵组织在多大程度上通过安全方法实现了上述每项收益？百分比反映选择显著实现或非常大程度实现的受访者（部分选项样本量较少）。

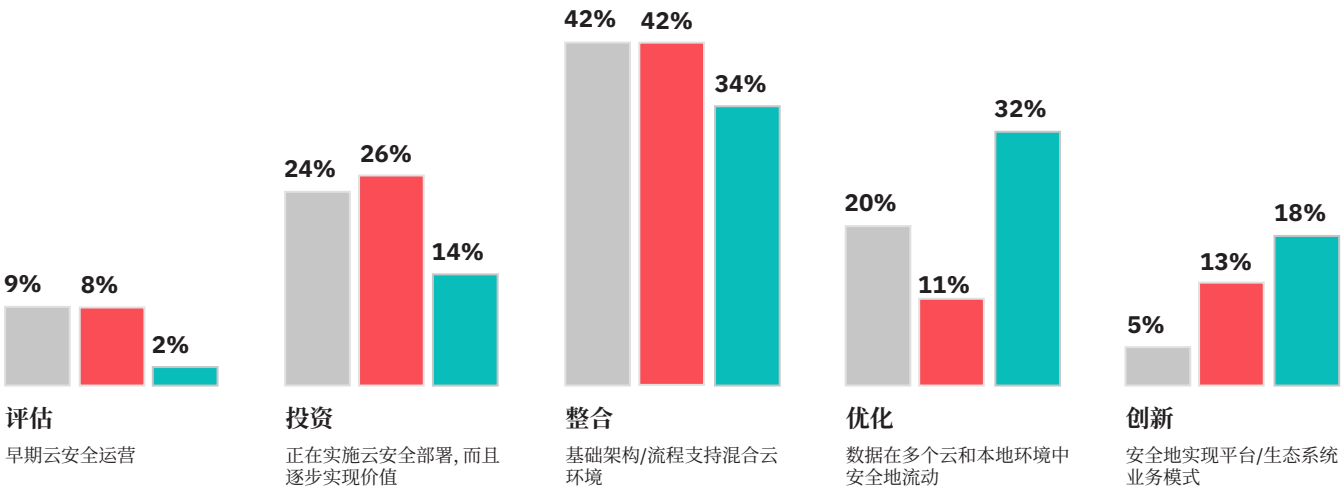
安全信息与事件管理 (SIEM)、安全编排与自动化响应 (SOAR) 以及 XDR 等指挥与自动化管理解决方案可提供整体威胁视图。这些解决方案通过结合企业数据、应用、网络和设备等上下文信息，深入揭示威胁，有助于加强安全调查，使率先尝新者能够更轻松地提高安全运营的敏捷性，并改善事件响应能力。

此外，零信任率先尝新者具备全面的云安全能力。1/3 的率先尝新者支持混合云环境，并能够充分利用在多个云和本地环境之间安全流动的数据。1/5 的率先尝新者则走得更远（见图 6）。他们能够可靠地实现新的云原生业务和运营能力，并将其扩展到内部和外部合作伙伴。

图 6

云优势

成熟的云安全能力支持新的平台业务模式



全球其他企业
中国企业
零信任率先尝新者

问题：以下哪项陈述最贴切地描述了贵组织云安全能力的成熟度？请选择一项（部分选项样本量较少）。

60% 的率先尝新者认为，他们的安全方法极大地促进了数字化转型；54% 认为，他们的安全方法增进了与外部合作伙伴的信任和安全联系。

什么让零信任率先尝新者真正地与众不同？那就是他们的网络弹性程度以及发挥运营效率和经济规模的能力。他们利用完整的云环境，与生态系统合作伙伴一起实现新的能力和业务模式。

尤其值得一提的是，一种率先尝新者实践可帮助组织实现更高的安全弹性和运营效率：

1. **实施指挥与自动化管理工具，以扩大零信任安全运营的范围和规模，提高可视性和效率：**
   - 使用生态系统范围的安全运营中心 (SOC) 以及协调的事件管理和危机响应能力，持续评估组织的安全态势。[9] 优先使用能够提供整个 SOC 可视性的工具。在所有本地和云环境中实现实时可视性，包括网络、设备、应用、用户和数据。这可以帮助决策者了解关键资产和服务的当前状态。
   - 部署覆盖多个云并与多个供应商的解决方案集成的安全解决方案。SOC 团队应具备与云提供商无关的一站式平台，提供任何云提供商环境的可视性，以便可以在生态系统中的任何地方随时调查任何基于云的事件。
   - 实施基于 AI 的安全智能，分析数据流以检测异常行为。结合来自多个领域以及外部来源的安全信息，以扩充互动的情境化数据/元数据，并实施安全策略。通过在各种云环境中应用相同的程序，扩展日志捕获能力，通过扫描发现可能表示数据泄露迹象的异常配置。

构成要素 3：部署零信任安全控制框架

零信任率先尝新者将零信任控制能力整合到现有的安全运营之中。他们使用安全遥测、实时流量分析以及指挥与自动化管理能力，提供更出色的安全洞察。

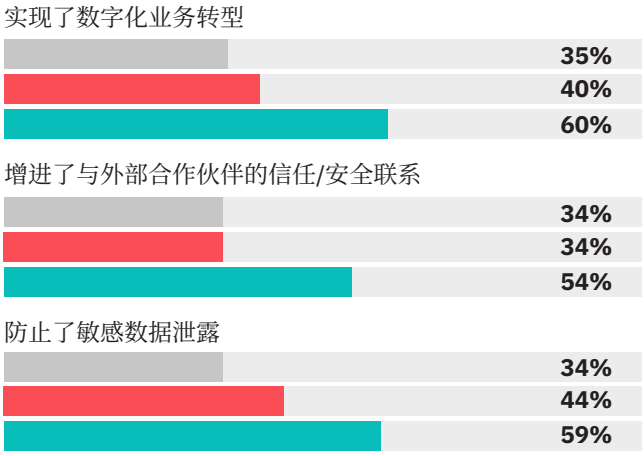
这涵盖了用户、设备、数据、网络和工作负载等关键资源。由于率先尝新者通常与生态系统合作伙伴协同运行这些资源，因此他们能够更有效地根据洞察采取行动。这也帮助增强了网络弹性，推动全新价值主张。

与之相关的收益显而易见。60% 的零信任率先尝新者认为，这种方法极大地促进了组织的数字化转型；54% 认为它加强了与外部合作伙伴的信任和安全连接（见图 7）。

图 7

信任的力量

零信任提高弹性并加强数字化转型工作



问题：贵组织在多大程度上通过安全方法实现了上述每项收益？百分比反映选择显著实现或非常大程度实现的受访者。

将信任转化为交易变量有助于增强运营环境的完整性。率先尝新者能够更全面深入地了解任务关键型资源，因此能够更高效地开展运营。通过在更靠近关键资源的地方部署安全控制，例如，围绕特定资产和服务创建微边界，他们可以扩展认证和验证控制，而不会带来不必要的摩擦。这样可以防止未经授权的访问和敏感数据泄露，从而增强弹性。

从整体上看，这种运营变化非常微妙，但意义重大。通过在预定义的区间建立信任 — 针对特定事件和行为使用验证和认证控制，信任协商就成为一种动态、实时的能力。由于信任可以根据情况或上下文环境调整，因此可以实现新形式的协作和价值交换。

构成要素 3

部署零信任安全控制框架

实现了数字化业务转型

60%
零信任率先尝新者

增进了与外部合作伙伴的信任与安全联系

54%
零信任率先尝新者

怎么做

- **加强网络和数据保护**
- **控制数据访问并管理数字身份**
- **规范云治理**
- **扩展对每个尝试访问关键资源的终端的可视性**
- **加强对工作负载的监督**

IBM 基于可扩展的开放系统，构建了一个零信任控制框架，提供集成化的服务和产品，保护数字化资产（见图 8）。

以下 5 种实践和相关活动对于建立零信任控制框架至关重要：

1. 增强网络和数据保护，首先建立分段网关，以实现更细颗粒度的访问控制：

– 使用下一代防火墙（NGFW）增强云安全控制。为 NGFW、电子邮件和云安全网关以及 DLP 解决方案定义规则和策略，以实施数据安全和访问策略。它们应该适用于各种托管模式、位置、用户和设备。

– 定期在本地、终端、传输过程和云端执行敏感数据发现与分类操作。捕获足够数量的数据与元数据，以便为任何特定的互动重新建立完整的上下文。

了解最敏感的数据所在的位置、谁可以访问（以及如何访问）、谁进行访问（以及何时访问）、他们用这些数据做什么。这样有助于满足数据隐私与合规标准，以及监控和控制对高度敏感数据的访问。

2. 通过控制数据访问和管理数字身份，加强用户保护：

– 定期检查用户访问权利。建立基于角色的数据访问控制。采用最小特权原则，根据公认的合法需求，访问执行特定任务所需的信息和资源。

向特权用户简要介绍相关的网络安全控制和实践。记录有权访问敏感资源的用户，然后监控行为并进行审计，以提高可视性，标记异常情况和潜在的恶意行为。

– 针对关键应用和数据资产实施多因子认证（MFA）。员工应使用双因子认证（2FA）或 MFA，以确定安全人员需要关注的领域，防止内部攻击。[10] 此外还应辅以特权身份管理（PIM）解决方案和强大的身份管理和治理（IMG）流程。

随着绕过 MFA 的技术的出现 — 尤其是对 OAuth 和 SAML 等信任机制的滥用，组织必须更加重视身份管理，将其作为漏洞的潜在来源。[11] 必须加强与凭证管理和秘密管理相关的策略与控制。

随着绕过认证的技术出现 — 尤其是滥用信任机制 — 组织需要将身份管理视为潜在的漏洞来源。

3

3. 建立正式的云治理流程，促进开放性和互操作性：

– 建立正式的云治理流程。在标准化治理策略和框架的基础上构建云治理模式，确保与云相关的安全支出有助于推动实现与云采用相关的业务目标。

– 建立针对云数据和工作负载的治理和监督机制。迁移到云端时，明确定义组织与云提供商的职责分配方式。

在责任共担模式下，提供商通常负责保护和管理基础架构，而客户负责保护在基础架构上运行的数据和工作负载。为了降低数据丢失和不遵守法规的风险，必须使用云提供商提供的专业安全服务。

4. 将可视性扩展到每个尝试访问关键资源的终端，加强设备保护和微边界：

– 在允许终端连接到企业 IT 网络或访问系统之前，对终端进行运行状况检查。使用自动化解决方案，扫描和记录新的终端设备。

向注册表添加新终端，以及详细说明相关用户、资源和事件的背景数据。发现和分析未经授权的用户和不受管理的设备，防止其获得访问权限。

5. 加强对工作负载的监督：

– 记录和监控工作负载配置。实施多云安全解决方案，提供对云平台实例、工作负载、配置设置、授权服务和凭证的集中监督。

图 8

IBM 的零信任控制框架

构成要素 4

开发具备强大适应能力的网络人才管理系统

零信任率先尝新者的网络人才保留率比同行高出 10%

60%
零信任率先尝新者

50%
所有其他企业

怎么做

聘用天赋异禀、态度明确以及经验丰富的人才：

培养持续学习和持续创新的企业文化，重视学习倾向

构成要素 4：开发具备强大适应能力的网络人才管理系统

无论组织选择如何实施零信任能力，如果没有高技能的网络人才资源，他们就难以长久保持安全和业务成果。[12] 但许多组织在招聘和留住这些技能方面存在困难。平均而言，用合格的求职者填补人才空缺需要 150 天。

为了应对这一挑战，零信任率先尝新者使用更为动态的网络人才管理系统，适应技能和需求的快速变化。最值得注意的是，他们认识到拥有具备学习能力的人才与拥有特定技能的人才同样重要，因此在招聘有潜力的人才方面也不遗余力。

由于众多组织争夺同一批高价值人才，因此那些拥有更深层次或更多样化人才库的组织具有决定性的优势。技能培养计划可以提供具备高潜质的人才，填补关键的空缺职位，帮助企业保持有效的安全态势。[13]

零信任率先尝新者将更高比例的网络安全预算用于打造持续学习的企业文化，积极培养网络资源技能。网络人才保留率可以反映这一点，他们的这个比例 (60%) 要比其他组织 (50%) 高出 10%。

两种实践有助于推动具有强大适应能力的网络人才管理系统：

1. **转变安全人才管理流程，专注于聘用天赋异禀、态度明确以及经验丰富的人才：**
   - 为每个网络安全职位定义技能、天赋和能力要求。结合更广泛的绩效管理目标，使经理能够更轻松地发现技能差距，以便通过招聘和培训计划来消除差距。考虑投资于人才解决方案，定期更新技能、职位和培养标准，使人才这一可变因素随着新技术和运营需求的发展而与时俱进。
   - 在招聘时，优先评估行为和能力，而不是经验。随着云的出现，安全事件的增加速度远远超出许多团队的管理能力。网络安全专业人员必须灵活地发展技能，以适应新出现的风险。他们还必须擅长与自动化安全解决方案协同工作。在应对新威胁方面，对战术、技术和业务流程的熟悉程度可能比网络安全运营经验更加重要。
   - 在候选人选拔过程中应用网络天赋测试以确定人才潜力。评估应聘成功的候选人的基本网络安全技能、态度和行为，然后利用这些洞察将潜在人才库扩展到安全组织以外。这样有助于提高员工队伍的多样性，引入新的思维方式，增加以不同方式应对挑战的选项。

培养一种不仅重视知识，而且重视学习倾向的企业文化。

4

2. 推动持续学习和持续创新的企业文化，培养和留住人才。以全新方式吸引人才，改进零信任安全运营：

- 为安全人员制定培训计划，学习业务的其他部分。提供有关关键业务流程的更深入的运营洞察，帮助他们更好地了解任何相关风险。
- 实施 AI 和其他工具，为整个人力资源生命周期内的持续学习工作提供信息。认可在招聘过程中发现的潜在人才，并通过定制化的学习和培养过程优化人才技能。这样可以让新员工迅速跟上进度，促进跨专业领域的团队合作，为候补人才库创建辅助资源池，并在新威胁和新技术出现时确保安全运营团队始终跟上步伐。
- 培养一种不仅重视知识，而且重视学习倾向的企业文化。提供专业发展和成长的机会，以提高员工保留率。为特定职位定义成功标准和职业道路。创建激励机制，鼓励顶尖人才分享自己的专业知识，与组织共同成长。

基于零信任思想的设计蓝图

根据零信任的主要原则，以及 IBM 在零信任方面的领域知识，结合客户在网络安全领域面临的主要挑战，我们设计了以下四个应用场景的整体蓝图，希望对不同企业基于零信任思想开展信息安全规划和建设有所启示。

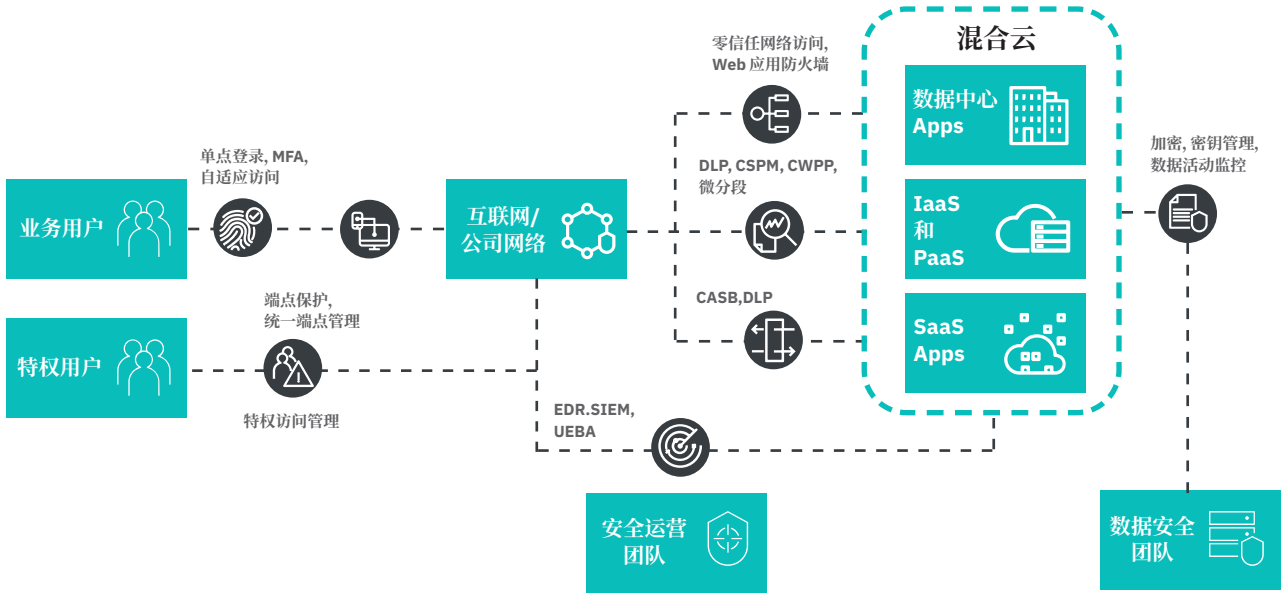
应用场景 1：保护混合云环境

数字化转型依赖于混合云，在所有云环境中统一、一致地部署安全能力，有助于提升业务运营的信心和弹性。

零信任方法可以帮助组织实现运营现代化，通过在业务中动态地适应用户、数据集和工作负载，无论它们运行在何处，使安全性成为业务连续性的保障。以零信任的方式保护混合云可以提供集中的可见性、安全上下文和统一管理，从而始终贯彻执行安全策略，帮助组织快速创新，拓展业务（见图 9）。

图 9

保护混合云环境的整体蓝图



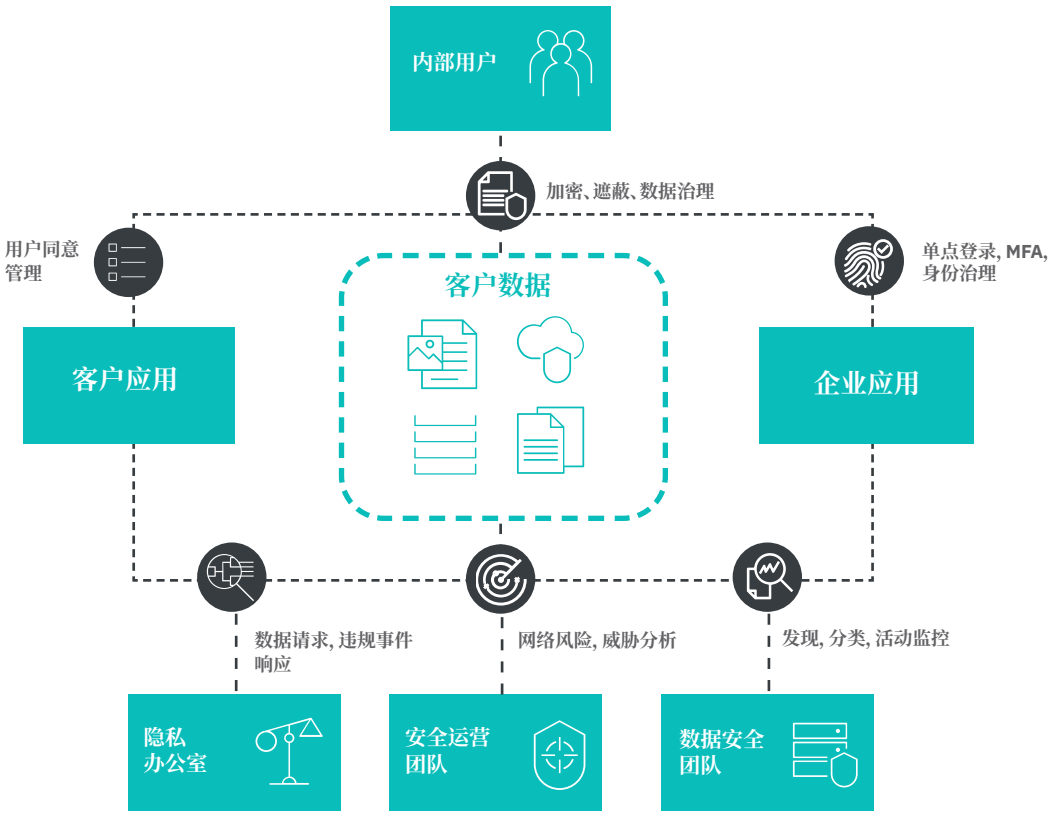
应用场景 2：保护客户隐私

对于个人隐私的保护在全球越来越受到重视，2018 年，欧盟 GDPR《General Data Protection Regulation》，即《通用数据保护条例》正式生效，2021 年，我国相继推出了《数据安全法》和《个人信息保护法》。确保隐私不仅仅是遵守法律和法规，它也是展示透明度和问责制的一个基本要素，有助于促进品牌信任。

零信任方法可以帮助组织通过基于最小特权的访问控制来保护客户隐私，只允许那些有合法需求并出于合规目的的用户访问请求。网络安全风险和威胁是不可避免的，组织需要具备快速检测、调查和响应潜在的客户数据泄露，特别是隐私数据。这有助于提升品牌的信誉度，增强客户的信心（见图 10）。

图 10

保护客户隐私的整体蓝图



应用场景 3: 降低业务中断和勒索软件的风险

像勒索软件这样的持续攻击会造成高昂的成本，对企业的数字化资产造成严重破坏。零信任的方法有助于隔离高价值的资源，降低安全风险。对于业务可能面临的威胁，零信任方法依据权限最小化，无永久特权等原则，依据动态策略进行安全控制，当威胁发生时，快速进行自动化响应（见图 11）。

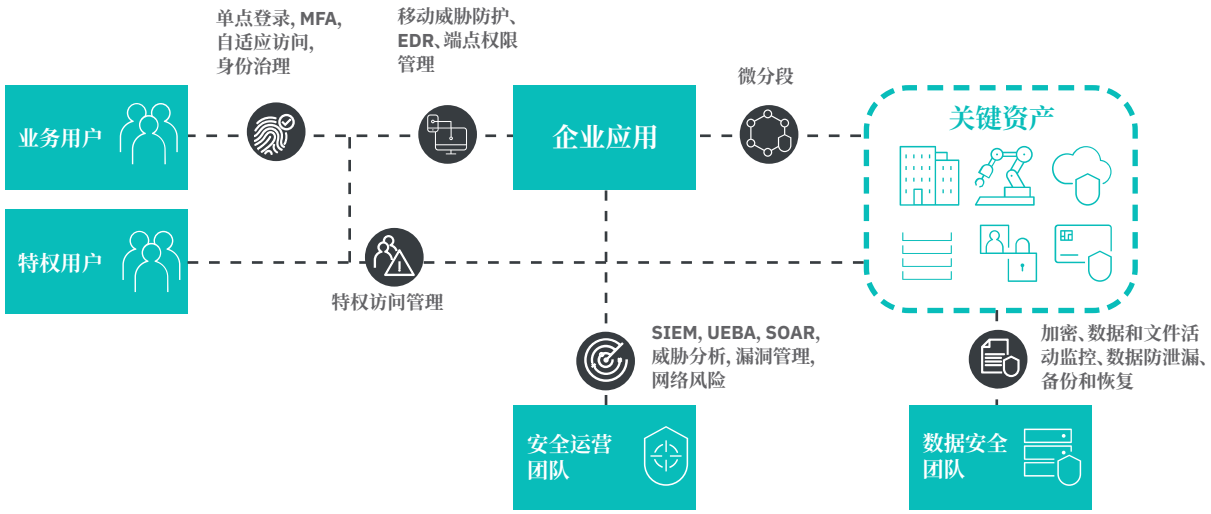
应用场景 4: 安全的远程办公环境

疫情以来，远程办公变为常态，员工可以使用任何设备，在任何位置，远程连接到多个环境中的数字化资源。

零信任方法可以帮助组织跨所有安全域关联安全信息，快速执行基于最小权限模型的基于条件的访问，从而为工作人员授权对资源的访问。在实现安全访问资源的情况下，不影响客户体验（见图 12）。

图 11

降低业务中断和勒索软件风险的整体蓝图



要成为零信任率先尝新者，需要考虑以下问题：

- 我们如何用零信任能力补充现有的安全架构?这种方法有何本质不同之处?为什么需要一种新方法?
- 组织通过哪些方法形成综合的威胁视图，以增强可视性、提高安全运营的敏捷性并改进事件响应能力?
- 我们如何在整个数字资产（包括网络、数据、用户、工作负载和设备）中纳入零信任控制?
- 我们可以通过哪些方式调整网络人才实践，以充分发挥零信任战略的作用?

研究方法

2020 年第四季度，IBM 商业价值研究院与牛津经济研究院合作，对来自不同地理区域和行业的 1000 多位运营和安全高管进行调研，其中 62 位来自于中国，以深入了解有效的零信任安全战略的内容以及如何实施零信任能力。

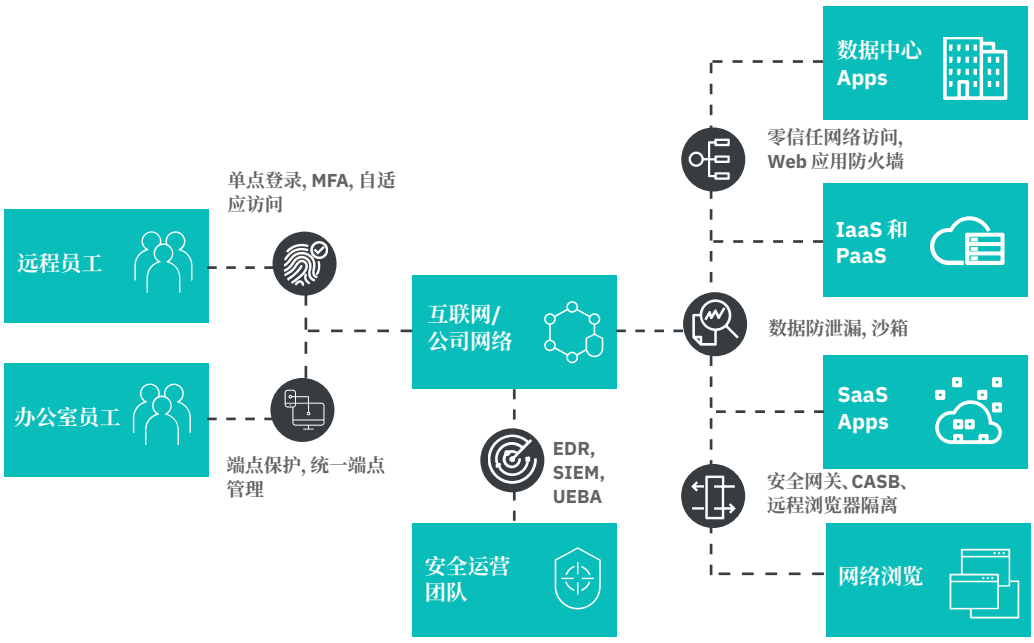
为了了解关键基础架构面临的威胁，本次调研收集了与 IT 和 OT 相关的网络安全风险数据，以及组织管理和消除这些风险的能力的成熟度、表现情况和有效性方面的数据。其中包括采用领先实践的情况，以及未来的优先任务与计划。我们在调研中还探讨了受访者从安全运营方法中获得的收益。

数据分析表明，23% 的组织在为了保护运营环境中的关键资源而实施零信任能力方面领先于同行，我们将其称为“零信任率先尝新者”。通过评估绩效指标和领先实践，我们得出结论，他们从这种方法获得了重要的业务和安全收益。

验证性因子分析 (CFA) 帮助我们深入了解推动实现收益的各种因素。这包括运营网络风险和安全实践；AI 驱动的分析和自动化；用于保护数据、网络、用户、设备和工作负载的零信任实践。由此，我们确定了基于 4 个基本构成要素和一套相互强化的实践的零信任运营方法。

图 12

安全远程办公环境的整体蓝图



关于作者

冯靓
IBM 大中华区科技事业部
网络安全业务总经理
emmafeng@cn.ibm.com

高爽
IBM 大中华区科技事业部
安全技术总监
gaos@cn.ibm.com

张炜
IBM 大中华区科技事业部
安全中国区销售总监
zhnwwei@cn.ibm.com

王莉
IBM 商业价值研究院
高级咨询经理
gbswangl@cn.ibm.com

Chris McCurdy
IBM Security Services
副总裁兼总经理
cmccurdy@us.ibm.com

Shue-Jane Thompson 博士
IBM Consulting
高级合伙人, 安全战略与发展杰出行业主管
shuejane@us.ibm.com

Lisa Fisher
IBM 商业价值研究院
工业、EE&U、T&T 与 MEA 全球对标分析研究主管
lfisher@za.ibm.com

Gerald Parham
IBM 商业价值研究院
安全和 CIO
全球研究主管
gparham@us.ibm.com

致谢

感谢以下同事对本文的贡献:叶亮

相关 IBV 报告

Gerald Parham、Shue-Jane Thomson、Shawn Dsouza 和 Shamla Naidoo 合著,“云安全的新时代: 利用信任网络, 增强网络弹性”,IBM 商业价值研究院, 2021 年 3 月 26 日。https://www.ibm.com/downloads/cas/LZ7MXO4M

Jim Comfort、Blaine Dolph、Steve Robinson、Lynn Kesterson-Townes 和 Anthony Marshall 合著,“混合云平台的优势”,IBM 商业价值研究院, 2020. https://www.ibm.com/downloads/cas/07LZOR5B

“2021 年 CEO 调研报告: 识别‘必需’: 制胜后疫情时代”, IBM 商业价值研究院, 2021. https://www.ibm.com/downloads/cas/QYVZMJ5N

Payraudeau、Jean-Stéphane、Anthony Marshall 和 Jacob Dencik 合著。“数字加速”,IBM 商业价值研究院, 2021. https://www.ibm.com/downloads/cas/ZB1KXDRL

选对合作伙伴, 驾驭多变的世界

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

IBM 商业价值研究院

IBM 商业价值研究院 (IBV) 站在技术与商业的交汇点, 将行业智库、主要学者和主题专家的专业知识与全球研究和绩效数据相结合, 提供可信的业务洞察。IBV 思想领导力组合包括深度研究、专家洞察、对标分析、绩效比较以及数据可视化, 支持各地区、各行业以及采用各种技术的企业做出明智的业务决策。

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

备注和参考资料

1 “IBM 2021 X-Force Threat Intelligence Index.” IBM Security. February 24, 2021. https://www.ibm.com/security/data-breach/threat-intelligence

2 “2021 数据泄露成本报告”. IBM Security. July 2021. https://www.ibm.com/downloads/cas/R1ZLBDPM

3 “IBM X-Force 威胁情报指数 2021 年”. IBM Security. February 2021. https://www.ibm.com/downloads/cas/1N6KEGVR

4 Marks, Joseph “The Cybersecurity 202: The Kaseya attack is a revolution in sophistication for ransomware hackers” *The Washington Post*. July 8, 2021. https://www.washingtonpost.com/politics/2021/07/08/cybersecurity-202-kaseya-attack-is-revolution-sophistication-ransomware-hackers/; Caltagirone, Sergio, Dr. Tom Winston, and Kyle O’Meara. “2020 ICS Cybersecurity Year in Review.” Dragos. https://www.dragos.com/year-in-review/

5 Kramer, Andrew E., Michael Schwirtz, and Anton Troianovski. “Secret Chats Show How Cybergang Became a Ransomware Powerhouse.” *The New York Times.* May 29, 2021. https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html

6 Osborne, Charlie. “Colonial Pipeline attack: Everything you need to know.” ZDNet (US Edition). May 13, 2021. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

7 郭倩. “个人信息保护法 11 月 1 日起实施”. 经济参考报. 2021 年 11 月 1 日. http://www.jjckb.cn/2021-11/01/c_1310282188.htm

8 Parham, Gerald, Shue-Jane Thomson, Shawn DeSouza, and Shamla Naidoo. “The new era of cloud security: Use trust networks to strengthen cyber resilience.” IBM Institute for Business Value. March 26, 2021. http://ibm.co/cloud-security-cyber-resilience

9 Ibid.

10 Pollard, Jeff and Stephanie Balaouras. “Craft Zero Trust Security Metrics That Matter - Performance Management: The Zero Trust Security Playbook.” Forrester. March 24, 2020. https://www.forrester.com/report/Craft+Zero+Trust+Security+Metrics+That+Matter/-/E-RES136188?objectid=RES136188

11 OAuth, or Open Authorization, is an authorization process. It allows third-party services to exchange user information without users having to give away their passwords. SAML, or Security Assertion Markup Language, is an authentication process. Both applications can be used for web single sign-on (SSO), but SAML tends to be specific to a user, while OAuth tends to be specific to an application. They are both required and work together.

12 Johnson, David, Samuel Stern, et al. “Focus On Employees’ Daily Journeys To Improve Employee Experience.” Forrester.April 20, 2018. https://www.forrester.com/report/Focus+On+Employees+Daily+Journeys+To+Improve+Employee+Experience/-/E-RES126042?objectid=RES126042

13 Parham, Gerald, Shue-Jane Thomson, Shawn DeSouza, and Shamla Naidoo.“The new era of cloud security: Use trust networks to strengthen cyber resilience.” IBM Institute for Business Value.March 26, 2021. http://ibm.co/cloud-security-cyber-resilience

关于研究洞察

研究洞察反映的是主管对于重要业务和相关技术主题的洞察。这些洞察是基于对绩效数据和其他对标分析结果进行研究分析而得出的。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com

IBM Corporation
New Orchard Road
Armonk, NY 10504
美国出品
2021 年 12 月

国际商业机器（中国）有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编：100101

BRLA2XP4-CNZH-00