研究洞察

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

IBM

IBM 如何提供帮助

IBM Security 可以帮助企业充满信心地向混合多云迁移，让上云之旅的每个阶段都安全无忧。如欲了解更多信息，请访问：ibm.com/security/ciso

扫码关注 IBM 商业价值研究院

官网　微博　微信公众号　微信小程序

作者：Shue-Jane Thompson 博士、Shamla Naidoo、Shawn DSouza 和 Gerald Parham

摘要

高管们认识新的风险和运营需求

如果仍沿用原来的安全模式，只是在此基础上不断扩展，那么会让已经非常紧张的能力、人才和预算问题进一步加剧。只有 35% 的首席信息安全官和 19% 的首席执行官认为自己的组织能够轻松吸引和留住必要的安全人才，以维持有效的安全态势。49% 的高管认为复杂性是影响其安全部门工作成效的最大障碍。

云环境要求安全方法 发生根本性转变

云环境的安全运营强调速度、规模、互操作性、自动化和协作。在云安全之旅中走得最远的组织使用自动化解决方案的比例，要比刚起步的组织高出 6 倍。前者在威胁缓解生命周期中的表现也要优于后者两倍。

安全从成本中心 转变为价值推动因素

80% 的受访最高层主管认为安全是组织的差异化品牌优势。具有最成熟云安全实践的组织的收入增长和盈利水平要比其他同行高出两倍以上。

号角已吹响

大多数高管都认同云安全非常重要。但究竟有多重要呢?

2020 年 12 月 17 日，美国网络安全与基础设施安全局 (CISA) 发布了有关通过 SolarWinds Orion 软件进行的有组织攻击的严重警告：“CISA 确认，这一威胁对联邦、州、各级地方政府，以及关键基础设施实体和其他私营组织带来了巨大风险。”[1]

在接下来的几周里，调查人员确定某个国家/地区的攻击者将 SUNSPOT 恶意软件植入 SolarWinds 的 Orion 软件更新之中，造成了名为 SUNBURST 的后门漏洞。[2] 这次攻击破坏了 SolarWinds 软件供应链的完整性，使其毫无觉察地将恶意软件当作常规软件更新的一部分传播到数以万计的政府和私营实体。

这些攻击者因此获得了访问特权，并利用它建立了进入其他系统的后门。[3] 虽然这起事件的完整影响范围可能要几个月甚至几年才能弄清楚，但它凸显了云生态系统核心的一个弱点：我们共同依赖于一个庞大的第三方供应商网络，但对关键提供商的安全状况缺乏了解。[4]

“这就好像你某天早上醒来，突然意识到，在过去 6 个月里，有个窃贼一直在你家进进出出。”曾在 2015 至 2020 年担任国家安全局总法律顾问的 Glenn Gerstell 这样表示道。[5]

虽然这次黑客攻击暴露出软件供应链和云生态系统中的严重漏洞，但也表明各组织需要携手合作，相互保护，基于运营和交易信任建立安全社区和弹性网络。与以往任何时候相比，安全愈发成为由多方共担责任的团队运动。事实上，这次黑客攻击的曝光也是受影响的公司、供应商和政府机构协作调查的结果。

81%

在最高管理层中，**81%** 的高管认为安全是让组织脱颖而出的品牌属性。

9400 万美元

CISO 和 CEO 对组织年度风险总成本的估算相差 **9400 万**美元。

超过 2 倍

在云安全实践方面最成熟的组织的收入增长和盈利水平要比同行高出**两倍以上**。

云安全难题

随着云生态系统日益成熟，这些平台、技术和服务既让云变得更加强大，但也成为漏洞的来源，这一趋势正变得越来越明显。安全主管越来越担心一个问题：如何确保在云端的投资取得成效？

IBM 商业价值研究院 (IBV) 在 2020 年 6 月进行的一项调研发现，将近 90% 的云开销用于公有云或混合云，40% 的总体工作负载在多云环境中运行。[6] 我们的安全运营方法必须适应这种实时协商安全边界和信任的新型工作方式。新冠病毒疫情和 SolarWinds 黑客事件的影响在领导们的脑海中挥之不去，他们认识到，每一次云对话都必须安全可靠。

本报告探讨云基础架构、技术和服务如何转变网络安全运营的方式。我们询问了来自 20 个国家或地区中 17 个行业的 930 位安全和业务领导，从两个角度评估他们的云运营状况（请参阅第 21 页的“研究方法”）。首先，他们的组织将业务运营迁移到云的速度有多快？第二，他们的云安全运营的相对成熟度如何？我们使用这些数据，更深入地了解云安全能力是否跟上了云迁移的步伐。

本报告的章节从三个角度介绍我们的调研结果：

- 了解风险
- 转变安全模式
- 重新构想安全，推动实现价值。

新冠病毒疫情促使数字化转型进程突然加速，也让这方面的投资显得更加迫切。

第 1 章：新能力，新风险

云迁移产生新的漏洞和攻击途径

由于新冠病毒疫情的影响，工作方式发生了巨大的变化，组织领导需要评估运营状况，探索开展业务的全新方式。新冠病毒疫情促使数字化转型进程突然加速，也让这方面的投资显得更加迫切。

向远程工作模式的转变是如此迅速而且出人意料，彰显出去中心化的云基础架构和云安全运营的优势。例如，在危机爆发之际，许多组织为实现灵活的工作环境，加大了多因子身份验证、零信任安全框架和安全策略的使用力度。

但是，在向云运营模式的转变过程中，也暴露出在数字化供应链和数字化运营的核心中，存在重大的依赖性和局限性，以及由此产生的风险。运营限制因素、*临时*远程工作安排以及意想不到的设备和接入点组合将企业暴露于新的风险之中。[7]

出于本次调研的目的，我们定义了云安全转型的五个阶段（见图 1）：

- *评估*。早期的云安全运营包括试点项目和/或有限的生产部署。为云安全确定候选用例、制定业务战略和/或构建价值案例。
- *投资*。正在实施云安全部署，而且逐步实现价值。制定战略和业务案例。
- *整合*。基础架构和流程确保数据在支持业务职能的各种云环境和本地环境之间安全流动。安全地启用基于云的新产品/新服务。
- *优化*。充分利用多个云和本地环境之间数据安全流动的优势。实现了云安全功能和效益。
- *创新*。能够可靠地抓住云原生业务和运营机遇，并将其扩展到内部和外部合作伙伴。运营反馈推动持续改进。

尽管毫无疑问，云的采用受业务目标的驱动，但安全问题和考虑因素在云转型工作中发挥着根本性的作用。对于大多数组织而言，云安全工作仍在路上。[8] IBV 2020 年的一项调研发现，只有 42% 的受访者表示，他们在整个 IT 基础架构中部署了多云安全与合规机制。[9]

图 1

转型阶段

首先，制定战略和业务案例，然后随着能力的逐步成熟，提高投资回报率

当战略、设计和治理等因素相互起到促进强化作用时，安全运营团队就能取得突破性的成果。

在本次调研中，受访高管表示，随着他们云“足迹”的不断扩大，面临的云风险也与日俱增（见图 2）；但随着组织的云安全成熟度不断提高，安全态势会逐渐改善（见图 3）。

这些调研结果表明，在云安全方面的投资正在收获回报，但也表明必须使运营和治理实践实现现代化，这对于保持有效的安全态势至关重要。

复杂性给安全部门带来挑战

49% 的受访高管认为，基础架构或运营的复杂性是他们面临的最严峻挑战。就目前而言，复杂性是安全部门工作成效所面临的主要障碍，这一点在调研中被提及的次数几乎是排名第二的因素的两倍。

值得注意的是，受访者提及的许多其他因素 — 比如缺乏人才 (22%)、治理问题 (22%)、缺乏技能 (20%)、缺乏运营一致性 (20%) 等，也可能反映出与复杂性相关的底层问题。

IDC 在 2019 年进行的一项调研表明，超过三分之一的组织从 16 个不同的供应商那里购买不少于 30 种云服务。[10] Forrester 最近的一项调研发现，复杂性会侵蚀投资回报 (ROI) 和阻碍创新，而解决复杂性问题则有助于提高组织的弹性。[11]

安全治理是最重要的设计考虑因素，无论其采用安全标准、管理策略还是控制框架等形式。表现出色的安全运营团队之所以能够脱颖而出，主要原因是他们采用创新方式减轻复杂性，以提高效率、一致性和运营质量。

图 2

阶段风险

随着越来越多的运营迁移到云端，与云相关的安全事件数的百分比也随之增加

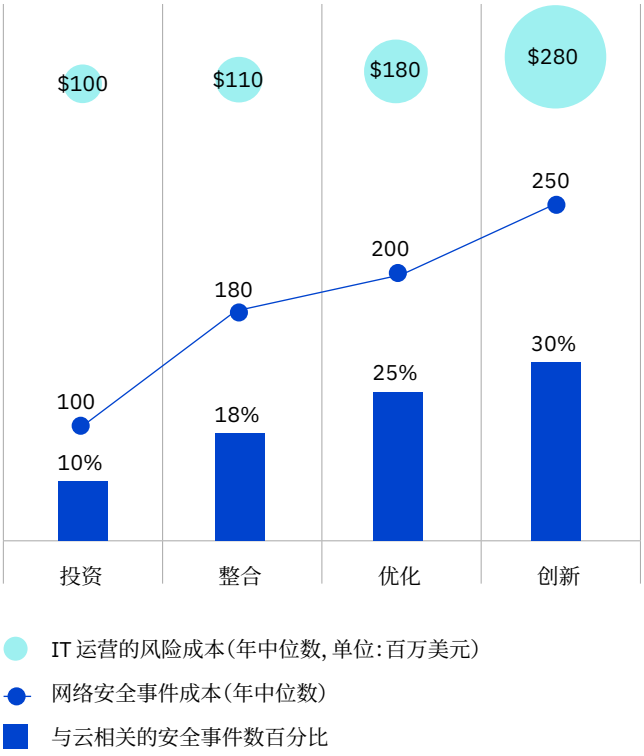
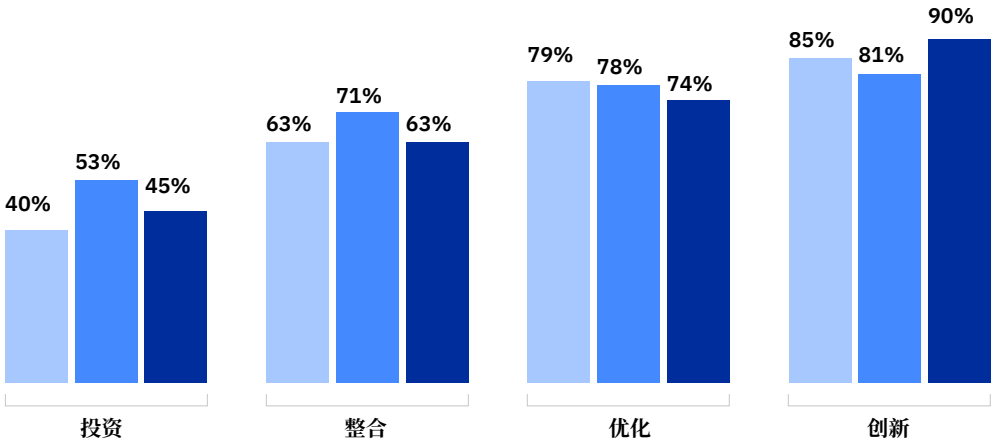


图 3

安全红利

随着组织不断增强云安全能力，安全态势也随之逐步改善



我们的云运营与安全态势保持一致
我们确保各个云供应商的环境保持一致的安全态势
我们能够实时了解安全事件以及它们如何影响整体安全态势

当战略、设计和治理等因素相互起到促进强化作用时，安全运营团队就能取得突破性的成果。在我们的调研样本中，一小组受访者充分体现了这种安全运营整体方法，我们称之为“云安全风向标”组织。

来自“风向标”群体的受访者表示，他们的收入增长和盈利水平都要超过其他同行两倍以上（分别为 86% 对 40% 和 84% 对 38%）。（请参阅“观点：云安全风向标组织转变安全模式。”

观点：云安全风向标组织转变安全模式

处于云迁移和安全发展早期阶段的组织可以向那些已经在云安全运营方面作出重大投资的组织学习。在我们的调研样本中，有 28% 的组织脱颖而出，在安全表现、技术熟练程度、运营敏捷性和云安全成熟度方面领先于同行，我们称之为“风向标”组织（见图 4）。

与其他同行相比，这些风向标组织在更大程度上整合了云与安全战略，这主要是因为他们在为混合多云环境做准备。这些组织针对云原生运营进行了优化，专为合作伙伴整合与协作进行了设计，并通过采用领先的实践和通用的治理机制，提高业务弹性。

因为他们已经克服了许多早期阶段的整合挑战，所以风向标组织可以指导其他同行如何实施全面的云安全项目。

随着成熟度逐步提高，行业风向标组织正想方设法借助以云为中心的安全能力，改善整体安全态势。他们开发了以责任共担、敏捷安全运营和简化的安全治理为中心的云原生安全运营模式。

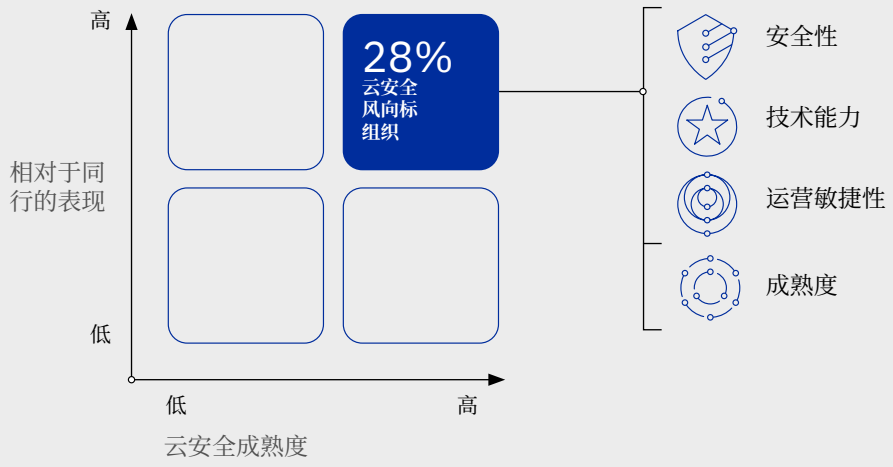
这些能力帮助风向标组织从数据中获得洞察，更有效地与合作伙伴开展合作。他们还在更广泛的网络产品组合中融入了新的价值主张。

风向标组织在四个重要方面脱颖而出（见图 7）。

图 4

脱颖而出

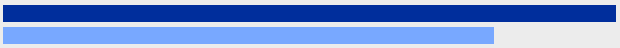
风向标组织在受访者中占 28%，他们在 4 个方面给自己给出高分



风向标组织 | 其他组织

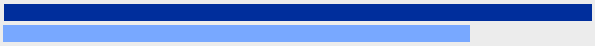
他们将网络风险、安全性、业务弹性与组织的核心使命联系在一起

96% | 77%



风向标组织在董事会级别影响组织战略

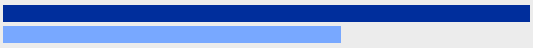
92% | 74%



风向标组织的安全运营团队明确定义了成功标准。

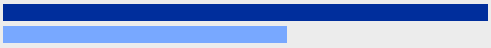
他们通过实现自动化，提升运营品量、规模和专业化水平

83% | 53%



风向标组织使用自动化技术来响应安全事件

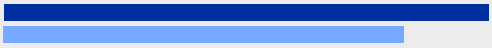
76% | 45%



风向标组织依靠机器学习和 AI 来加强安全运营

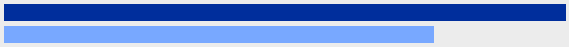
他们优先考虑运营敏捷性，帮助生成洞察

76% | 63%



风向标组织通常将安全遥测技术整合到数据分析中

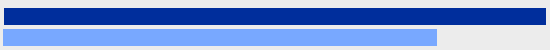
88% | 67%



风向标组织通过简化和标准化技术工具集，增强安全态势

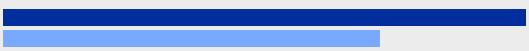
他们与合作伙伴携手整合安全运营

85% | 68%



风向标组织让所有云供应商的环境保持一致的安全态势

82% | 59%



风向标组织能够全面了解合作伙伴的供应链

如果在设计中考虑安全性，IT 基础架构和运营的下游复杂性就会降低。

新方法：安全左移

让统一的安全功能成为产品和服务设计中不可分割的一部分，而非事后再考虑安全要求，这种方法有时称为“安全左移”。如果安全功能成为设计的必要考虑因素 — 确保以更安全、更透明的方式开展业务，我们就能够有效降低 IT 基础架构和运营的下游复杂性。

同样，像 DevOps 和 DevSecOps 这样的云原生运营模式也越来越受欢迎，因为这些模式以一种整体的方法处理开发、配置和支持，将它们作为相互依赖的变量（见图 5）。DevOps 整合了软件开发、部署和支持职能，实现持续集成与交付 (CI/CD) 能力。DevSecOps 是对 DevOps 的改进，确保将安全能力整合到开发与交付生命周期中。

零信任安全模式明确地将信任转化为一种运营变量，进一步扩大了安全保护伞的范围 — 使用访问控制、上下文数据以及风险/信任评分，阻止网络中未经管理的数据移动。如果与身份管理解决方案集成，零信任设计就可以实现个性化而且高度安全的互动。

但必须记住，新的应用、服务或运营能力本身并不能提供更出色的安全性；就算提供了安全性，它们也可能带来新的风险，让安全环境更加复杂。除非安全运营和治理实践也实现现代化，否则迁移到云安全应用平台将事倍功半。当然，这说起来容易做起来难。首席信息安全官 (CISO) 目前面临的最大挑战之一就是如何平衡业务需求与安全运营问题。

领导层就战略和优先任务存在分歧

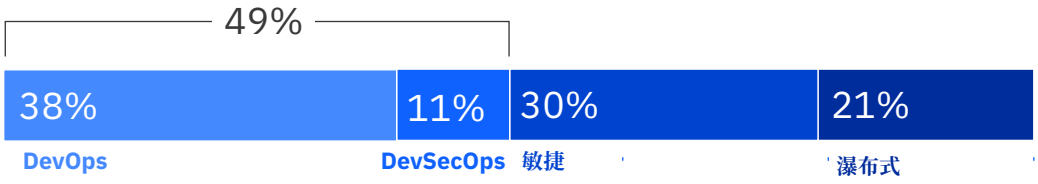
即便是那些声称自己在云安全实践方面最成熟的组织，也不能始终保持一致的安全态势。在最为成熟的组织中（处于“优化”和“创新”阶段），有将近五分之一的受访者不认为自己的云运营与企业的安全态势保持一致，或者对此不置可否。超过五分之一受访者不认为他们能够让所有云提供商的产品或服务保持一致的安全态势，或者对此不置可否。

我们发现不同职位的高管也对整个组织安全运营的观点不一。乍一看，领导对自己组织的技术和安全战略的看法似乎是一致的：91% 的 CISO 表示，组织的云和安全战略“严丝合缝”，而 80% 的 CEO 也对此表示同意。然而表象之下隐藏着分歧。

图 5

安全第一

49% 的受访者现在使用 DevOps 和 DevSecOps，将安全能力整合到 IT 基础架构和运营中



四分之三的 CISO 表示，组织的云运营与安全态势保持一致，而只有 62% 的 CEO 同意这种说法。同样，对组织的云安全路线图表示出信心的 CEO 的比例（69%）明显低于 CISO（92%）。尽管 CISO 和 CEO 都表示组织的云和安全战略保持同步，但上述调研结果表明存在明显的认识差距。

对于处在云转型过程中的组织（即*大多数*组织）而言，这些观点上的差异可能会深刻影响正在进行的安全现代化工作。

与 CEO 相比，CISO 计算的安全违规成本要高出 40%（CISO 计算的每次违规平均成本为 360 万美元，CEO 计算的则是 260 万美元），而且他们报告的每年安全违规次数也要多出 20%（CISO 报告每年平均 65 次，CEO 报告 54 次）。这些差异让组织每年的风险敞口成本总额相差令人惊讶的 9400 万美元。

我们不禁要问：是什么导致了这种差异，安全运营和业务战略之间的脱节对运营有何影响？如果众多 CEO 确实低估了组织 IT 风险的频率和程度，可能会影响到风险管理之外的某些关键领域的行政决策，比如安全预算和人员配备。

此外，尽管由于高管的职责不同，在认识上有所差异是可以理解的，但这些差异往往导致他们在优先任务问题上产生分歧，反映在安全决策*患得患失*、预算需求存在观点冲突，或者董事会对安全问题缺乏了解、职责不清。

最重要的是，由于高管的认识不一致，往往导致核心关切和根本原因成为最后解决也是最难解决的问题 — 这种后果可能会对组织的整体安全态势产生深刻影响。

这些洞察表明，安全领导和业务领导必须就风险和价值进行更深入的对话。如果能够协同部署云和安全方面的创新成果，就能够显著降低风险，形成新的价值主张，有效增强业务弹性。请参阅侧边栏“福特汽车公司：通过现代化推动创新、加快速度和增强弹性。”

福特汽车公司：通过现代化推动创新、加快速度和增强弹性[12]

福特汽车公司是制造安全可靠、技术先进的汽车的全球领先者。他们的使命是以可接受的价格，为客户（包括向各种零售和商业消费者进行销售的经销商和零部件分销商）提供出行解决方案。

“我们是知名品牌。Ford oval 几乎家喻户晓。”福特汽车公司产品服务负责人 Jason Presnell 说道，“我们的使命是成为一家出行公司，不仅要找到帮助人们出行的新方法，还要为他们提供旅行所需的信息和工具，比如用于发动或解锁汽车的移动应用。我们需要在全球范围内支持和提供这些能力。”

福特的业务部门管理着一个强大而踊跃的开发社区。但是，成千上万的员工以及数以千计的内部应用和站点之间的协作，造成了福特的传统 IT 环境和开发方法无法适应的复杂性。此外，该公司还面临着与支持原有环境相关的人力成本居高不下的问题。因此，福特希望建立一种基于容器的云原生新环境，帮助其更有效地利用资源，并加强安全监管。

福特打算在数据中心内使用容器技术、应用编程接口 (API) 和自动化技术，对原有应用进行现代化改造，从而改善安全性，提高自动化程度，并优化硬件、软件和资源的比例。最终，福特采用了基于 Kubernetes 的容器管理解决方案。福特还与一家管理安全服务提供商合作，旨在提高开发和生产环境的可视性、降低风险并加强保护。

借助新的多租户云容器环境，福特的经销商和工厂运营方可以更快地访问新的功能、修订包和更新。现在，许多面向关键工作负载的流程大幅增速；借助“容器即服务”所提供的支持，福特的生产力也得到显著提高。采用基于容器的方法只需较少的初期硬件投资。此外，由于福特继续对传统应用进行现代化和迁移，因此还持续实现成本节省。

第 2 章：
重新思考安全运营

光靠扩展现有的安全模式，无法适应云安全运营的要求

如果云会产生新的漏洞 — 就像刚开启云安全之旅的组织经常会遇到的情况那样，那么扩大现有的安全运营实践可能会让目前的资源、技能和能力紧张状况雪上加霜。这是因为，现有的安全运营模式并不是为云原生变量而设计的 — 这些变量包括速度、规模、互操作性、自动化、不断变化的服务组合，以及与组织外的合作伙伴共担的安全责任（见图 6）。这些变量中的任何一个都会对安全运营带来新的压力。而云环境要求同时考虑所有这些变量。

在云运营中，网络边界和特权访问等传统安全实践得到增强，加入了端点感知、多因子身份验证、实时数据/元数据分析和自动化策略管理等新能力。这代表了一种深刻的变化。无论是消费者体验还是商业智能，云安全服务正逐渐成为产生价值的必要条件。云安全的作用不仅仅是保护云；还是业务支持的核心部分。

图 6

原有环境在哪些方面滞后

传统的安全运营无法利用云原生能力

传统安全运营	→	云安全运营
规划周期较长 部署和补丁计划频率较低：事后添加安全功能	→	**敏捷运营** 迭代冲刺、响应迅捷的决策、在设计中考虑安全治理
大型单体式应用 复杂、不易扩展、难以更新	→	**开放标准和可互操作的服务** 易于升级的模块化 API 和微服务
许多手动流程 能力限制和技能缺乏限制了灵活性	→	**高度自动化和强大感知能力** 基于实时洞察和自动响应能力的 CI/CD
孤岛式的目标 单独的开发、安全和运营团队	→	**DevSecOps** 整合的运营、支持和治理，改善安全成果
成本中心与价值创造脱节 安全性依靠组织完全拥有和运营的解决方案独立运行	→	**共享价值和共担责任** 安全职责相互依存，由生态系统合作伙伴社区共同维持

不断变化、多方协作是混合多云安全运营独有的特点

生态系统发展：围绕共担责任模式重新定位

也许云安全运营模式中最重要的变化是新的协同工作方式。传统的安全运营模式假定组织能够完全了解自己所拥有和运营的安全平台。而云安全则基于更为分布式的运营模式，其安全服务整合了众多资产、数据存储和供应商。

鉴于云安全运营的规模和速度，因此为了保持网络弹性，参与方必须迅捷地进行响应和沟通、共同解决问题以及敏捷地作出决策。这就需要基于责任共担原则建立新的安全治理模式。

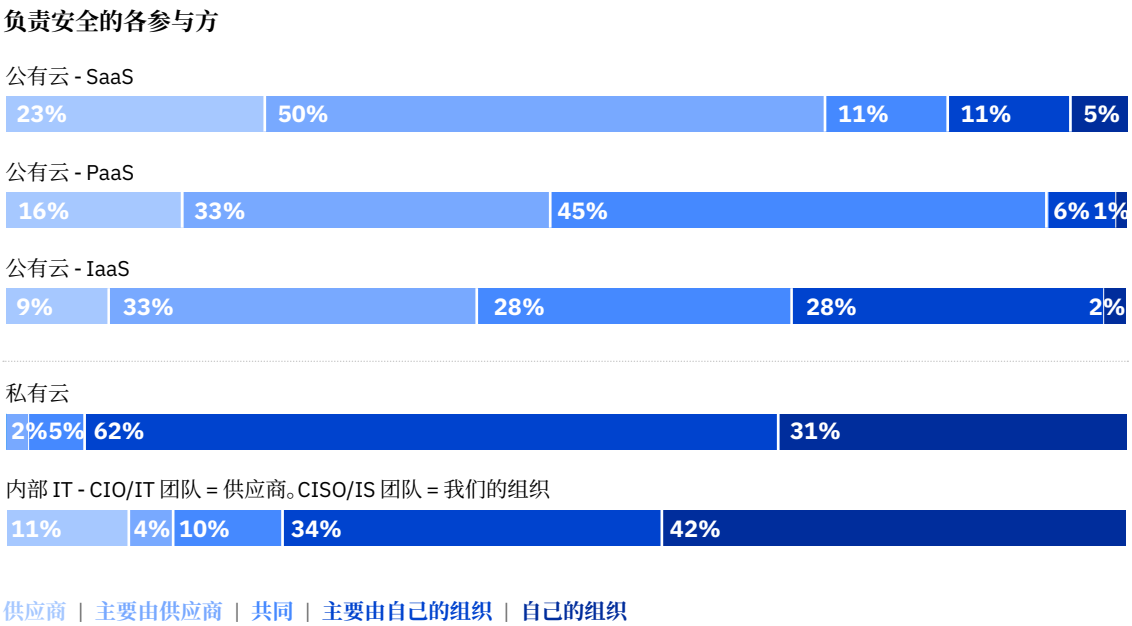
不断变化、多方协作以及有关各自责任的连锁协议是混合多云安全运营独有的特点（见图 7）。这涉及一系列广泛的能力，包括管理安全服务、专有的供应商洞察和专门的人工智能 (AI) 服务和基础架构级别的服务，例如遥测和日志捕获服务等。

借助标准设计模式提高合作伙伴的可用性，凸显出云安全的一个关键优势：通过实现应用和基础架构标准化，供应商可以提供增值安全服务，作为其核心云功能的扩展。事实上，本次调研发现，66% 的高管希望云供应商能够提供基准水平的安全能力。

图 7

共担责任

不断变化、多方协作是混合多云安全运营的特点



问题：贵组织如何分配保护以下技术基础架构的责任？

由于云安全性基于沟通、协作和共识，因此 CISO 必须将关注重点转移到人际关系技能上。

重新思考安全领导：CISO 的作用必须与时俱进

作为安全价值主张的主要支持者，CISO 必须能够清晰阐明与组织更广泛的业务目标保持一致的安全战略。最重要的是，CISO 必须能够自由地开展更广泛的网络安全对话，涉及网络弹性、数据完整性、运营信任和隐私等主题，而不是仅限于数据违规防范。责任共担模式是云安全不可或缺的组成部分，这意味着，CISO 需要更重视业务咨询、运营洞察、协作和创新。

每个运营多云环境的组织（目前的大多数组织都是如此）必须确保让众多云服务供应商提供的各种不同的运行时环境保持一致的安全态势。[13] 足有 70% 的受访者表示，他们需要衡量、监控和保护多个公有云和私有云供应商的工作负载，而 72% 的受访者表示，他们的组织需要让不同供应商的环境保持一致的安全态势。

因此，CISO 的角色需要进行调整，以满足这些需求。随着对第三方供应商的依赖程度日益提高，组织将一些基础架构和平台需求外包出去。但是他们并没有考虑到必须让各种联合服务、分布式运营以及经常存在矛盾的治理方法保持一致的安全态势。[15]

此外，组织越来越依赖数据洞察和自动化，这意味着，目前的安全领导必须具备最新的技术技能，以及开展协作式安全实践所需的人际关系与沟通技能。[16]

由于安全成果取决于一系列范围广泛的因素，因此 CISO 的领导技能变得比以往任何时候都更为重要。此外，由于这些成果基于沟通、协作与共识，因此 CISO 还必须改进人际关系技能，在组织内外建立承诺。

重新思考人才战略：用 AI 和自动化增强能力与技能

通过采用与要攻击的组织相同的云原生能力，如今的威胁制造者正变得更加无所不能，而且难以捉摸。鉴于攻击面不断扩大，以及业务运营日益加速，即使最优秀的安全运营团队也感到举步维艰。运营的复杂性进一步提高了风险，因为通常需要人类对补救措施进行判断。随着越来越多的运营迁移到云端，安全事件成倍增加，但组织却越来越难以找到并聘用技能高超的安全分析师。

持续的资源、技能和能力短缺可能发展为严重的风险因素。[17] 在我们的调研中，CISO 和 CEO 都认识到资源限制正在影响他们保持稳定安全态势的能力。只有三分之一的 CISO 和五分之一的 CEO 认为自己的组织能够轻松吸引和留住保持有效安全态势所需的安全人才。

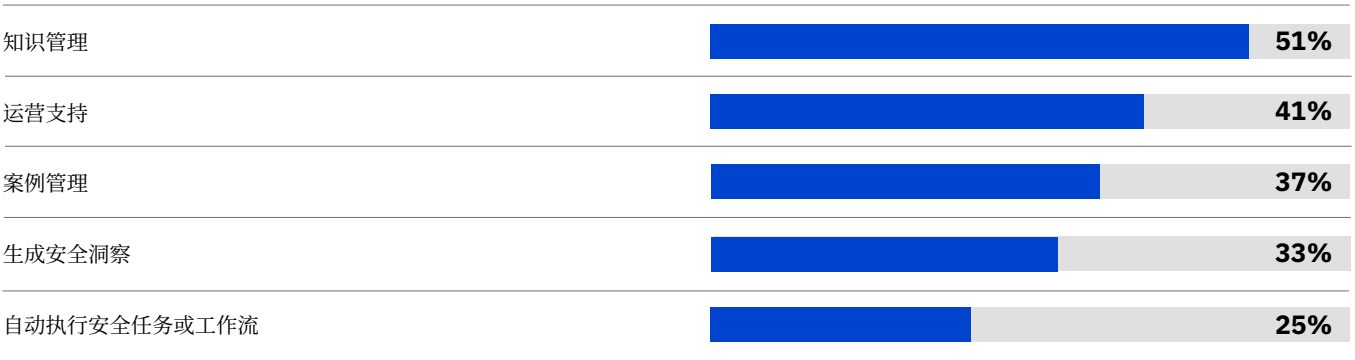
但基于云的安全性也带来许多颇有前景的机遇，其中之一就是自动化服务、基于 AI 的虚拟客服和高技能分析人员之间开展协作的可能性。AI 和机器学习技术在安全人才支持功能（如知识库、案例管理、运营洞察和自动化）方面发挥着日益重要的作用（见图 8）。这些技术可以有效补充和扩展高技能分析人员的能力，比如帮助整理数据、减少认知负荷或加速分析。

在实践中，这些工具为安全运营团队带来了额外能力。通过将领导从日常行政工作中解放出来，例如与呈指数级增长的设备和数据相关的任务，[17,18] 他们就可以集中精力吸引和留住更专业化的安全运营人才，从而对安全成果产生最大影响。[19]

图 8

技术支持人才

AI 和机器学习技术扩展了高技能安全分析师可以自行完成的工作范围



问题：贵组织的安全运营多大程度上整合了以下人工智能 (AI) 和机器学习 (ML) 能力（百分比）？

云生态系统的未来：基于社区的安全性

考虑到协作和责任共担的重要性，基于云的安全服务的兴起可能是安全运营领域最重要的趋势，这有助于促进供应商之间的互操作性和统筹协调。为了实现规模化并促进自动化，服务强调通用标准、模块化、透明度和责任。

示例包括开源库、众包软件开发工具和威胁情报共享。[20] 这些独立的社区在贡献专业知识、开发新的设计模式和倡导基于社区的安全治理标准方面发挥了关键作用。

随着混合多云成为标准模式，技术和安全领导要求服务能够帮助提高运营效率和弹性，而不是增加复杂性。开放式安全框架提供了一个机遇，让安全性摆脱专有和孤立的牢笼。关键的第一步是建立强大的社区，以帮助培养未来人才，围绕共同标准协调各方的工作，精简运营以促进协作 — 这些也都是增强网络弹性的关键步骤。

开放式安全框架将社区验证的设计与社区驱动的反馈以及基于社区的支持结合在一起。这种方法鼓励参与、共享、标准化和简化。在安全战略方面，开放式云设计的优点在于将复杂的运营变量（包括硬件、软件、配置和支持）转化为一系列标准化的服务，这些服务可在不同的云和不同的供应商环境中交付和管理。

此外，基于社区的网络安全方法势在必行，因为潜在的对手已采取这种方法来开展威胁活动。例如，“网络犯罪即服务”和非法市场共享先进的恶意软件资产和间谍情报技术。[21]

对于云解决方案供应商而言，能够按需增加能力、人员支持或专业知识是其主要的卖点之一。

第 3 章：云安全价值主张

大力对云投资，改善安全状况

随着越来越多的工作负载迁移到云端，以及云环境本身不断发展以支持更广泛的工作负载，在云安全方面做出最大努力的企业在威胁补救能力方面取得了长足的进步。

最成熟组织的表现要超过最不成熟组织两倍，对于处于云安全初始阶段的组织而言，累计的平均发现时间和平均遏制时间分别为 125 天和 250 天（见图 9）。在评估自动化能力时也发现了类似的模式：表示使用安全自动化能力的最成熟组织几乎是最不成熟组织 6 倍。

云生态系统合作伙伴的主要优点之一在于，他们能够提供其他人无法给予的东西 — 也就是运营超大规模的云原生业务所需的资源、专业化能力和基础架构。对于云解决方案供应商而言，能够按需增加能力、人员支持或专业知识是其主要的卖点之一。这既适用于专业化的云安全供应商，同时也更普遍地适用于提供安全服务的超大规模云供应商。

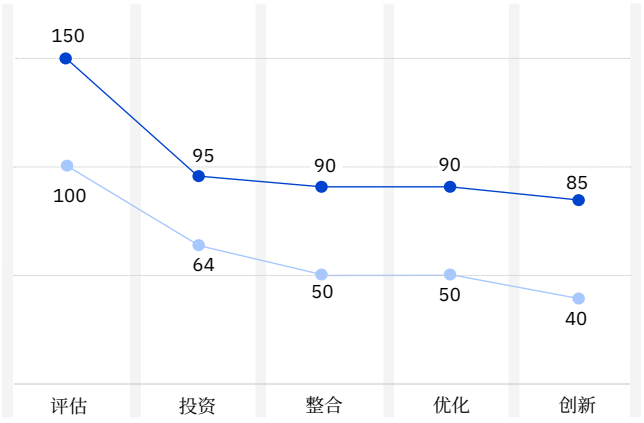
云基础架构和运营的整合使灵活性、能力、标准化和专业化有机融为一体，这是提高安全成果的关键所在。通过与合作伙伴合作，采用通用的安全运营和治理方法，并正确地决定哪些能力自己开发，哪些能力通过采购获得，组织甚至可在高度动态的运营环境中保持有效的安全态势。

图 9

威胁补救

借助更成熟的云安全能力，可以更快地发现和遏制威胁

威胁补救 KPI（按云安全阶段）



数据违规 — 平均发现时间，单位：天
数据违规 — 平均遏制时间，单位：天

利用安全投资，改善业务成果

然而在过去，安全性仅仅被狭义地视为“威胁补救措施”，而现在，人们对此的看法正在发生改变。企业范围的领导认识到，安全性是企业品质的重要组成部分。超过 80% 的受访者认同：安全、保证和信任是组织实现差异化的主要品牌属性。同样，83% 的受访者表示，安全能力为组织的产品和服务带来了更大的价值；87% 的受访者表示，安全性已整合到日常运营之中，是企业文化的重要组成部分。

安全领域内外的领导都赞同这些观点。组织的最高管理层 — 不仅是 CISO 和 CIO，还有 CEO 和 COO — 都有一个共识，那就是安全价值主张在不断扩大，这在很大程度上是由于云基础架构和服务实现了新的能力。

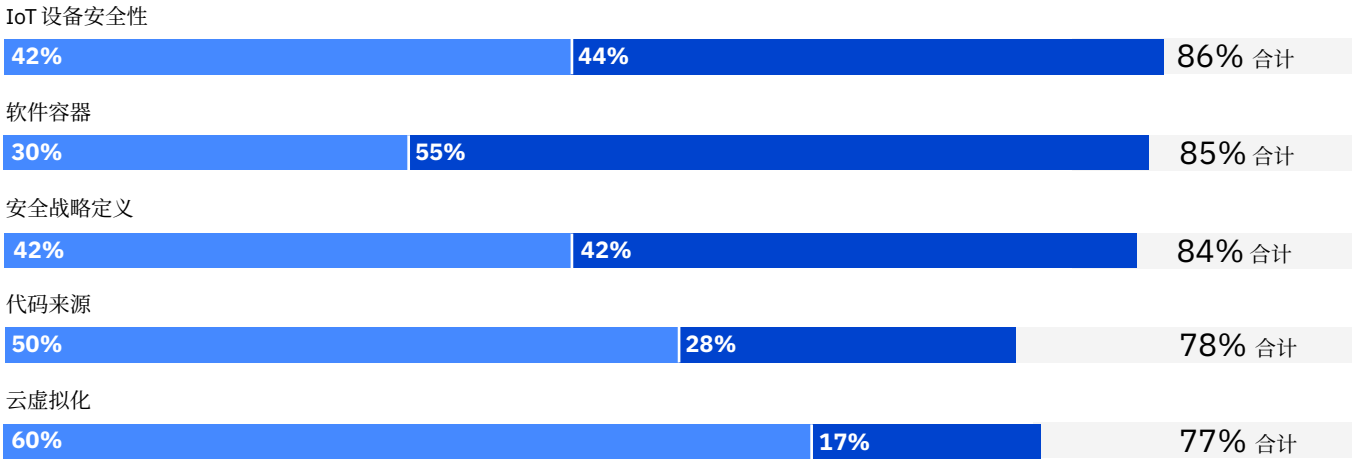
展望未来，云技术可能成为安全产品与服务组合中几乎所有创新的基础。组织正在确定各种能力的开发优先顺序，包括物联网设备安全性、软件容器、安全策略管理、软件供应链，等等（见图 10）。

因此，CISO 与技术同行（例如 CIO 和 CTO）的合作至关重要。这也凸显出 CISO 不仅在支持安全运营方面发挥着日益重要的作用，而且在新的运营能力和新的价值主张方面也更有话语权。

图 10

投资于创新

云技术带来了一系列有助于增强安全性的能力



组织范围的能力 | 核心组织能力（差异化优势）

注：图中显示选择答案 4 或 5 的受访者占比。问题：未来两年内，您预计以下每种能力将在贵组织的云安全态势中将发挥什么作用？
1 - 不起作用；2 - 概念验证/试验；3 - 限于地理区域或职能领域的的辅助作用；
4 - 组织范围的能力；5 - 核心组织能力（差异化优势）

使用协作式安全模式，增强网络弹性

为了应对不断扩大的威胁形势，安全运营正从传统上以缓解威胁为重点转变为更关注于网络弹性等整体问题。网络弹性作为一系列旨在增强企业整体安全态势的连锁能力，以全面和系统的方式满足整个安全生命周期的要求。

正如 Ponemon Institute 所描述的那样："具有高度网络弹性的企业以一种整体方式，成功地将连续性管理和灾难恢复与安全运营结合起来。"[22] 范围不断扩大的安全能力也是云安全价值主张的核心。

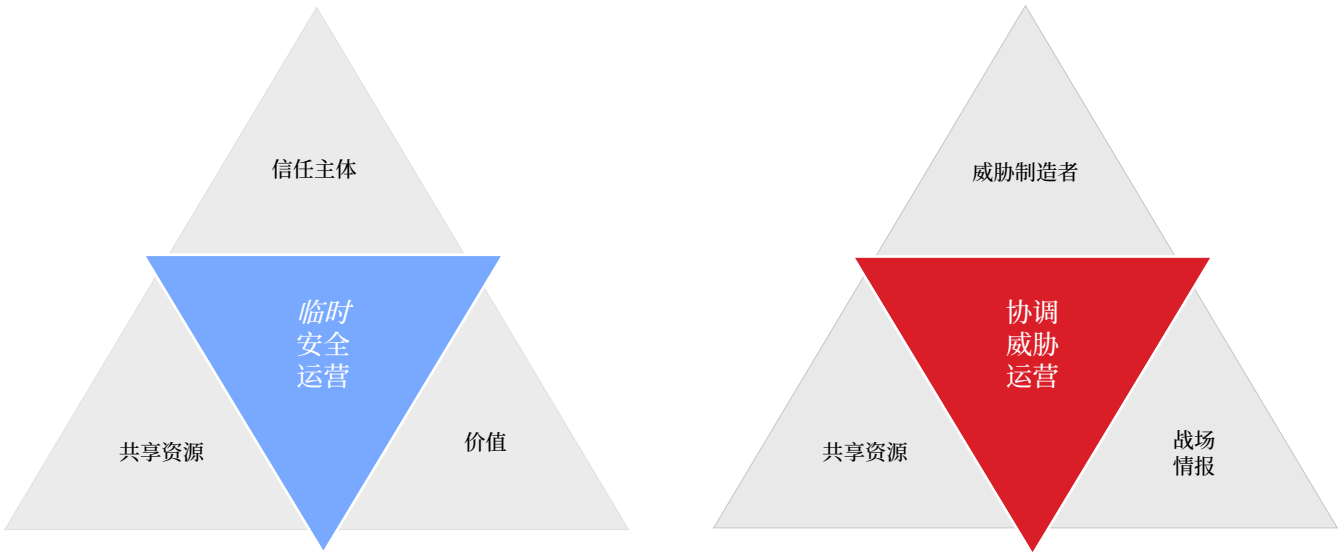
随着向以云为中心的运营模式的转变，不同合作伙伴的数据和运营日益联合在一起。威胁制造者也瞄准了战略合作伙伴，因此，威胁目标从单个组织扩大到共享生态系统。

目前，由于威胁可视性非常有限，因此云生态系统很容易受到攻击（见图 11）。信任主体通过共享资源来创造价值。但他们通常在事后，*临时*根据需要分享洞察或治理。威胁制造者则利用这些缺口来探查漏洞并破坏信任。他们协调行动，共享信息，最大程度利用漏洞实施攻击对于信任主体来说，如果整个生态系统缺乏网络意识和响应能力，则会降低网络弹性，并让实现价值的努力面临风险。

图 11

当前：网络军备竞赛

威胁制造者利用生态系统层面的漏洞发动攻击，这需要各参与方进行临时补救



通过以社区形式重构安全运营，同样是动态变化的环境，原本会给组织带来更多漏洞，而现在则有助于提高组织的安全性与弹性。

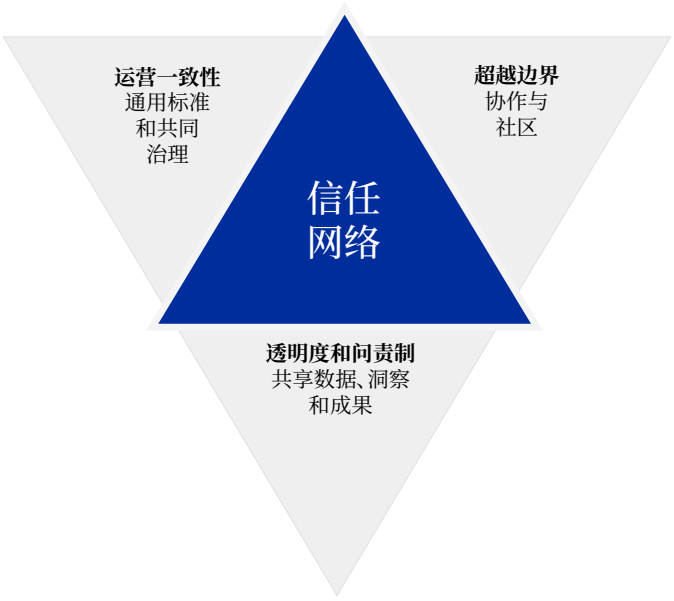
但是，如果领导将注意力转向责任共担模式，就有可能出现新的机会（见图 12）。通过将生态系统视为基于共同投资和共同承诺的社区，信任主体就可以从信息共享和合作中受益。在传统的生态系统中，企业边界充当断点，而缺乏威胁可视性可能会给整个生态系统带来共同的风险。

而在信任网络中，由多方（即集体）参与的安全性已成为常态。整个供应链与合作伙伴网络共担责任。随着时间的推移，许多方法整合为一体。因此，所有参与方都能够从增强的网络意识和网络弹性中受益。

图 12

未来：信任网络的优势

在整个生态系统中加强问责制和信息共享有助于增强所有参与方的网络弹性



就像坏蛋在暗网上协调行动、共享信息和资源一样，组织领导也可以选择对运营进行重新定位，以提高透明度、问责制和信任度，以便能够与可信网络合作伙伴分享洞察，扩大运营。

- 通过以社区形式重构安全运营，同样是动态变化的环境，原本会给组织带来更大风险和漏洞，而现在则有助于提高组织的安全性与弹性。
- 通过携手合作，生态系统可以将复杂性与碎片化等缺点转化为专业化和规模化等优势。
- 通过优先安排可视性、共享和共同治理等任务，领导就打开了超越组织边界的新价值主张的大门。

最后，云安全对于实现和扩展与网络安全领域相邻的新运营能力至关重要。例如，网络风险、供应链完整性、身份管理和运营信任都是有助于提高整体网络弹性的关键实践领域。

尽管市场动态仍在不断发展变化，但其意义十分明确：网络安全不再只是成本中心；它正在成为价值推动因素 — 83% 的受访者都认同此观点。

让每一次云对话都成为安全对话

为了适应后疫情时期的环境，我们可能需要从不同的角度重新审视业务关系和组织。在这种新常态下，云生态系统将越来越多地利用社区导向的协作式方法来实现安全性。

因此，第一步是了解云生态系统的宗旨 — 为可信合作伙伴提供可信的运营环境。通过综合云原生能力、在产能方面的共同投资以及协作式的安全治理机制，云生态系统就能够自然而然地转变为可信网络。通过坚持让每一次对话都成为安全对话，领导可逐步将对话的主题从安全意识转变为网络弹性。

通过将战略和设计考虑因素放在首位，基于云的可信网络就为携手合作与创造价值的全新方式打开了大门。当领导为云安全之旅的下一阶段做准备时，这些机遇可以让企业脱颖而出。

行动指南

云安全的新时代

帮助组织将云安全生态系统转变为可信网络的六条原则。

了解风险

1. 采用云与安全运营相结合的统一战略	– 评估安全战略是否以及多大程度上成为组织战略的扩展。 – 确保最高层领导对漏洞和风险具有相似的看法。
2. 确保安全运营实现现代化，与云投资保持同步	– 使用标准化衡量指标，最好是与合作伙伴一致的指标，客观评估云风险。 – 简化运营，消除摩擦和复杂性。
3. 重新构想安全性，实现责任共担，成果共享	– 打破内部和外部边界，全面审视风险。 – 使用公共治理框架，与生态系统合作伙伴一起对风险分类、沟通和威胁补救能力进行标准化。
4. 利用智能技术，满足云安全运营需求	– 评估云原生变量的影响，这些变量包括规模、速度、互操作性、自动化、不断变化的内外部服务组合以及共担的责任。 – 记录会影响风险状况和安全态势并且是组织所特有的云和安全因素。
5. 专注于业务弹性，重新定义网络安全的价值主张	– 使用风险建模和风险量化，理解与各种运营场景（如供应商或供应链受到攻击）相关的影响和可能性。 – 估算事件发生前、中、后保持网络弹性和业务连续性的财务成本。
6. 将安全性视为一个社区，利用它来增强信任	– 制定衡量指标，用于监控和改善整个生态系统的安全协作、共担的责任以及整体弹性。 – 将安全意识转化为企业文化问题，扩展到整个组织范围以及组织边界之外。

转变安全模式

1. 采用云与安全运营相结合的统一战略	– 通过评估组织层面的机遇和风险，制定自己的云安全战略。 – 制定统一的云和安全路线图，将组织目标、云运营能力、组织的风险状况和期望的安全态势联系在一起。
2. 确保安全运营实现现代化，与云投资保持同步	– 整合平台，实现产品和服务标准化，促进内部和外部协作。 – 将安全性整合到运营和支持生命周期 (DevSecOps) 中。
3. 重新构想安全性，实现责任共担，成果共享	– 创造性地思考如何让治理实践易于采用。 – 自动执行安全策略管理和安全控制框架。 – 通过提高可视性、共享信息和汇集专门资源，调查供应链攻击活动，缩小攻击面。

4. 利用智能技术，满足云安全运营需求	– 对运营进行重新定位，能够根据洞察（如遥测数据、分析、取证、威胁情报服务）生成并采取行动。 – 使用 AI 和自动化技术为分析人员赋能，获得更深入的洞察，改善安全成果。
5. 专注于业务弹性，重新定义网络安全的价值主张	– 集思广益，确定安全运营如何从开放合作和基于社区的安全框架中受益。 – 开发更具协作性的安全运营模式，针对多个云合作伙伴共享的服务进行优化。 – 采用公共治理框架，对风险和威胁分类模式进行标准化，协调运营实践，将安全能力扩展到组织边界之外。
6. 将安全性视为一个社区，利用它来增强信任	– 将内部和外部合作伙伴整合到安全模拟中。演练复杂场景，包括零日攻击、勒索软件和持久的高级威胁。 – 创建具有协调的事件管理/危机响应能力的全生态系统安全运营中心 (SOC)。

重新构想安全，推动实现价值

1. 采用云与安全运营相结合的统一战略	– 清晰地阐明安全性如何创造核心品牌价值，并强调业务弹性在保护品牌资本方面的作用。 – 证明安全运营以及安全周边的运营如何为实现同事的业务目标和业务结果做出贡献。
2. 确保安全运营实现现代化，与云投资保持同步	– 对投资条件和回报阈值进行标准化，然后选择哪些方面要进行专门化处理，哪些方面一般化处理即可。 – 采用适用于所有云提供商的开放式安全解决方案。
3. 重新构想安全性，实现责任共担，成果共享	– 让安全意识和信息共享成为企业文化惯例（“安全是团队活动”） – 投资人才与合作关系，帮助组织扩大规模，实现差异化优势。
4. 利用智能技术，满足云安全运营需求	– 让安全观点成为战略规划、产品开发和创新工作中不可分割的一部分（“左移”）。 – 让安全控制成为理所当然的事情（零信任），消除摩擦。 – 向同行学习。思考同行组织如何与时俱进，不断开发和改进其云安全能力。
5. 专注于业务弹性，重新定义网络安全的价值主张	– 记录网络安全在价值创造过程中所做出的贡献 — 例如，作为锚点，支持多方安全运营；作为载体，以新方式与内外合作伙伴开展合作；或作为渠道，加强诚信、透明和信任的品牌价值。 – 探索云生态系统在哪些方面已经在发挥信任网络的作用。
6. 将安全性视为一个社区，利用它来增强信任	– 评估如何将人才、技能和能力差距转化为共同创造、合作和专业化等方面的机遇。 – 通过共享资源、专业知识和信息，充分利用生态系统合作伙伴的广度和深度。 – 选择开放式安全解决方案，优化人才库、互操作性和可扩展性。

关于作者

Shue-Jane Thompson 博士
linkedin.com/in/shuejane
shuejane@us.ibm.com

Shue-Jane Thompson 博士是 IBM 全球企业咨询服务部安全战略与发展服务线的副总裁兼高级合伙人。她负责全球 170 多个国家或地区的客户的网络安全解决方案创新、整合、服务销售与交付。Thompson 博士在学术、商业、政府和国际技术和业务管理等领域拥有超过 30 年的丰富经验，赢得和管理过许多大规模的 IT、网络、云和任务运营项目。

Shamla Naidoo
shamla@us.ibm.com

Shamla Naidoo 是 IBM Security 的副总裁兼管理合伙人。Shamla 在多个行业的技术、安全和隐私领域拥有 38 年的工作经验。作为管理合伙人，她负责为首席执行官、董事会董事和其他最高层主管提供建议，指导他们如何将安全和隐私融入数字和业务转型战略之中。她曾担任过 IBM 的全球首席信息安全官，负责保护 IBM 的品牌、声誉和知识产权。

Shawn DSouza
linkedin.com/in/shawndsouza
shawn.dsouza@us.ibm.com

Shawn Dsouza 是混合云服务团队的全球首席技术官，该团度负责 GBS 中价值 100 亿美元的业务，为全球客户提供云转型和管理服务。Shawn 领导着一个由杰出工程师和技术负责人组成的全球团队，负责定义技术和指导发展方向，开发技术资产和加速器，帮助 GBS 和 IBM 在混合多云领域实现差异化优势。他在高管领导、咨询、云应用工程和软件产品开发方面拥有超过 22 年的丰富经验。

Gerald Parham
linkedin.com/in/gerryparham
gparham@us.ibm.com

Gerald Parham 是 IBM 商业价值研究院负责安全和 CIO 领域的全球研究主管。Gerald 的研究重点是安全战略和网络价值链，尤其侧重研究战略、风险、安全运营、身份管理、隐私和信任之间的关系。他在高管领导、创新和知识产权开发领域拥有 20 多年的丰富经验。

研究方法

2019 年底，IBM 商业价值研究院 (IBV) 与牛津经济研究院合作，对来自 20 个国家或地区中 17 个行业的 930 位高管开展了一次调研，旨在更深入地了解云基础架构、技术和服务如何影响受访者所在组织的安全态势。受访者包括所在组织中网络安全领域的负责人（CISO 和高级信息安全主管），以及其他与组织的安全领导（CISO、CTO、COO 和 CEO）直接合作的最高层领导。

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 “Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations.” Cybersecurity and Infrastructure Security Agency. December 17, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-352a

2 “JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA).” Cybersecurity and Infrastructure Security Agency. January 5, 2021. https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure; Bing, Christopher, Jack Stubbs, Raphael Satter, and Joseph Menn. “Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources.” Reuters. February 2, 2021. https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive-idUSKBN2A22K8

3 Jensen, Benjamin, Brandon Valeriano, and Mark Montgomery. “The Strategic Implications of SolarWinds.” Lawfare. December 18, 2020. https://www.lawfareblog.com/strategic-implications-solarwinds

4 Satter, Raphael, Christopher Bing, and Joseph Menn. “Hackers used SolarWinds’ dominance against it in sprawling spy campaign.” Reuters. December 15, 2020. https://www.reuters.com/article/us-global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idUKKBN28P2N8; Jensen, Benjamin, Brandon Valeriano, and Mark Montgomery. “The Strategic Implications of SolarWinds.”Lawfare. December 18, 2020.https://www.lawfareblog.com/strategic-implications-solarwinds

5 Chappell, Bill, Greg Myre, and Laurel Wamsley. “What We Know About Russia’s Alleged Hack Of The U.S. Government And Tech Companies.” NPR. December 21, 2020. https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little

6 Comfort, Jim et al. “The hybrid cloud platform advantage” IBM Institute for Business Value. https://ibm.co/hybrid-cloud-platform

7 Whitmore. Wendi and Gerald Parham. “COVID-19 cyberwar: How to protect your business.” IBM Institute for Business Value. https://ibm.co/covid-19-cyberwar

8 Robinson, Teri. “The cloud divide: Risks and rewards for companies that moved pre-pandemic.” SC Magazine. February 1, 2021. https://www.scmagazine.com/home/security-news/cloud-security/the-cloud-divide-risks-and-rewards-for-companies-that-moved-pre-pandemic

9 Comfort, Jim et al. “The hybrid cloud platform advantage” IBM Institute for Business Value. https://ibm.co/hybrid-cloud-platform

10 IBM press release. “IBM: Security in the Cloud Remains Challenged by Complexity and Shadow IT—New Data Pinpoints Top Security Risks for Companies to Address as Cloud Migration Accelerates.” June 20, 2020. https://newsroom.ibm.com/2020-06-10-IBM-Security-in-the-Cloud-Remains-Challenged-by-Complexity-and-Shadow-IT

11 Forrester. “Complexity In Cybersecurity Report 2019: How Reducing Complexity Leads To Better Security Outcomes.” May 2019. https://www.ibm.com/downloads/cas/QK1YD49A

12 “Ford Motor Company optimizes delivery with cloud platform.” RedHat. 2020. https://www.redhat.com/en/success-stories/ford-motor-company

13 Comfort, Jim et al. “The hybrid cloud platform advantage.” IBM Institute for Business Value. https://www.ibm.com/thought-leadership/institute-business-value/report/hybrid-cloud-platform

14 Nguyen-Duy. Jonathan. “Managing Today’s Risks Demands A Security Fabric Approach.” Accessed June 14, 2020. https://www.csoonline.com/article/3233293/managing-today-s-risks-demands-a-security-fabric-approach.html

15 Dotson, Chris. “Practical Cloud Security.” O’Reilly Media Inc. March 2019. https://www.oreilly.com/library/view/practical-cloud-security/9781492037507

16 Ikeda, Kazuaki, Dave Zaharchuk, and Anthony Marshall. “Three keys to competitiveness in an era of economic uncertainty.” IBM Institute for Business Value. https://ibm.co/IBV_economiccomp

17 Foster, Mark. “Building the Cognitive Enterprise: Nine Action Areas (Deep Dive).” IBM Institute for Business Value. https://www.ibm.com/thought-leadership/institute-business-value/report/build-cognitive-enterprise; Wright et al. “Accelerating the journey to HR 3.0.” IBM Institute for Business Value. https://www.ibm.com/thought-leadership/institute-business-value/report/hr-3; La Prade et al. “The enterprise guide to closing the skills gap.”IBM Institute for Business Value.https://www.ibm.com/thought-leadership/institute-business-value/report/closing-skills-gap

18 Radichel, Teri. “Exponential increases in cyber risk from Internet exposure.” Accessed June 14, 2020. https://medium.com/cloud-security/exponential-increases-in-cyber-risk-from-internet-exposure-124be0f43bf5; Business Insider Intelligence. “The security and privacy issues that come with the Internet of Things.” Accessed June 14, 2020. https://www.businessinsider.com/iot-security-privacy; Figure 7 - IoT vulnerabilities have increased 5400% over the last five years. “The 2019 Threat Intelligence Index.” IBM X-Force Red Vulnerability Database. Accessed September 10, 2020. https://www.ibm.com/security/data-breach/threat-intelligence

19 Crumpler, William, and James Andrew Lewis. “The Cybersecurity Workforce Gap.” The Center for Strategic & International Studies. Accessed February 22, 2021 https://www.csis.org/analysis/cybersecurity-workforce-gap

20 Sawers, Paul. “CodeSandbox launches Team Pro for whole product teams to collaborate on code in the cloud.” VentureBeat. Accessed February 22, 2021 https://venturebeat.com/2021/02/05/codesandbox-launches-team-pro-for-whole-product-teams-to-collaborate-on-code-in-the-cloud

21 Huang. Keman, Michael Siegel and Stuart Madnick. “Cybercrime-as-a-Service: Identifying Control Points to Disrupt.” Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management. Massachusetts Institute of Technology. November 2017. Accessed on June 12, 2020. http://web.mit.edu/smadnick/www/wp/2017-17.pdf; “Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar.” November 2019. Public-Private Analytic Exchange Program, sponsored by the Department of Homeland Security’s Office of Intelligence and Analysis on behalf of the Office of the Director of National Intelligence. Accessed on June 12, 2020. https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf

22 “The 2019 Cyber Resilient Organization.”Ponemon Institute and IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

关于研究洞察

研究洞察致力于为业务主管就公共和私营领域的关键问题提供基于事实的战略洞察。洞察根据对自身主要研究调查的分析结果得出。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com

IBM Corporation
New Orchard Road
Armonk, NY 10504
美国出品
2021 年 3 月

国际商业机器中国有限公司
北京市朝阳区北四环中路 27 号
盘古大观写字楼 25 层
邮编：100101

32038232CNZH-00