

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 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

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

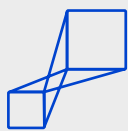
“这就好像你某天早上醒来,突然意识到,在过去 6 个月里,有个窃贼一直在你家进进出出。”曾在 2015 至 2020 年担任国家安全局总法律顾问的 Glenn Gerstell 这样表示道。⁵

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。

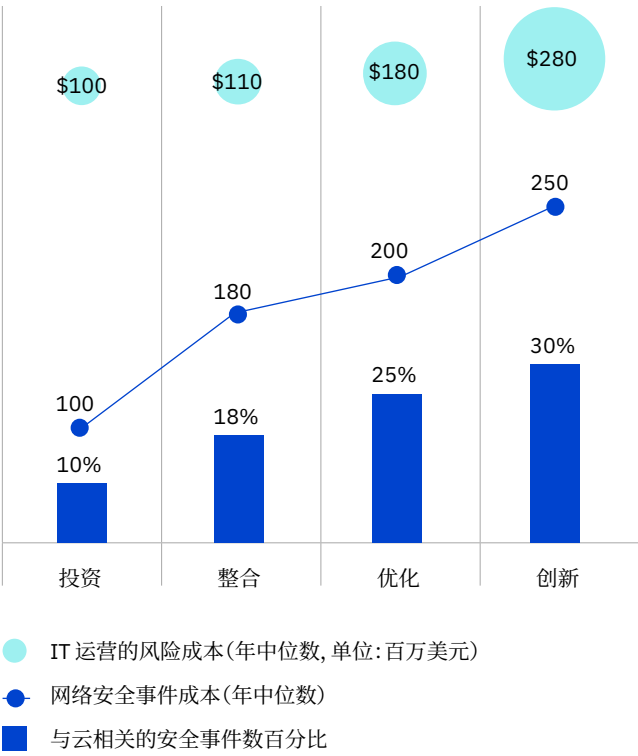
IDC 在 2019 年进行的一项调研表明,超过三分之一的组织从 16 个不同的供应商那里购买不少于 30 种云服务。¹⁰ Forrester 最近的一项调研发现,复杂性会侵蚀投资回报 (ROI) 和阻碍创新,而解决复杂性问题则有助于提高组织的弹性。¹¹

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

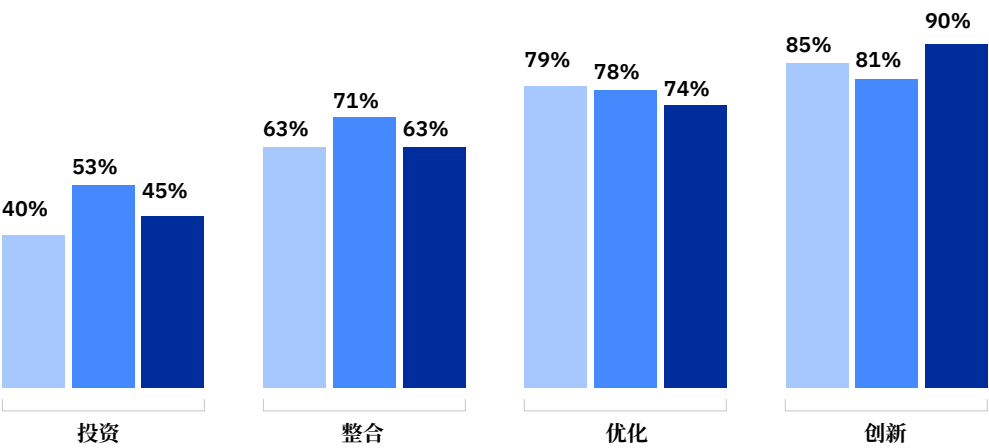


—

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。

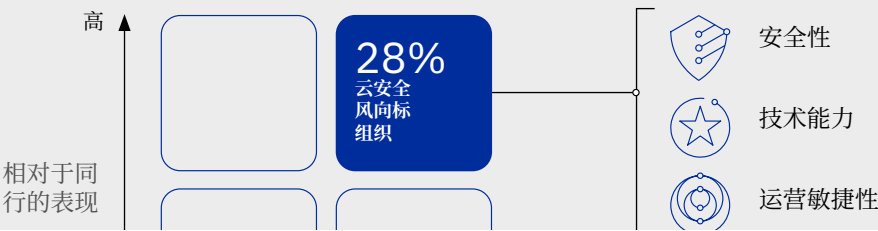
这些能力帮助风向标组织从数据中获得洞察,更有效地与合作伙伴开展合作。他们还在更广泛的网络产品组合中融入了新的价值主张。

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



预览已结束,完整报告链接和二维码如下:

https://www.yunbaogao.cn/report/index/report?reportId=1_46745

