veeam Insights

混合云和多云现状

2024

《2024 年数据保护趋势报告》

研究简报

目录

导言

每年，我们都会委托独立研究公司对负责组织数据保护策略的 IT 领导者和实施者进行调查。本年度研究的一个重要内容是了解各组织在 IT 团队努力简化业务流程时所采用的混合云和多云架构策略。尽管新冠疫情爆发后的头几个月，云采用率显著加速，但随后的四年，数据中心、私有云和多个公有云中的工作负载分布相对稳定。

2024 年，组织表示近一半的生产负载将在公有云中运行，其余部分将在数据中心内的物理服务器和虚拟机之间平均分配。

在过去几十年的 IT 格局中，人们从未见过可供选择的“黄金标准”生产平台的多样性。在过去，一流的数据中心几乎完全依赖于 Novell NetWare 或 Windows Server 基础架构，后者后来被 VMware、Hyper-V 和其他虚拟机管理程序的虚拟化基础架构所取代。在过去几代技术中，从昔日的首选平台真正迁移到新平台的情况并不少见，他们都选择了一种将新平台（如 Veeam for VMware）与各种云环境相匹配的最佳数据保护解决方案。

2024 年，尽管数据中心将继续为各种规模的企业提供关键 IT 服务，但以下情况并不少见：

- 利用 Azure、AWS、Google 和其他基础架构云
- 为文件共享或数据库采用专用基础架构服务
- 以及利用 Microsoft 365 或 Salesforce 等主流 SaaS 平台

您估计贵组织在 2024 年采用以下每种形式的服务器比例是多少？

27% 数据中心内的虚拟机

28% 数据中心内的物理服务器

45% “超大规模”或服务提供商 (MSP) 内的云托管服务器实例

鉴于云服务的关注度空前高涨，人们很容易认为现代数据中心的重要性正在减弱，但这是不正确的。相反，数据表明，大多数组织都采用“云智能”策略，即默认情况下新工作负载会考虑云托管，这反过来又削弱了仍由数据中心提供的 IT 服务比例，而这些工作负载实际上并没有从这些物理设施中迁移出来。

此外，业务流程和经济考量影响将托管在内部或异地的工作负载变得越来越普遍。事实上，即使在每个云端，我们也不能想当然地认为“云端之旅”是单向的，也不能认定“云端之旅”仅限于一个服务提供商。相反，能够在数据中心和云之间、云端之间流畅地移动工作负载的业务需求带来了机遇和挑战。

对于都面临着领导组织实施“智能云”战略的迫切任务的三个关键利益相关者，本研究简报将为他们提供数据和见解：

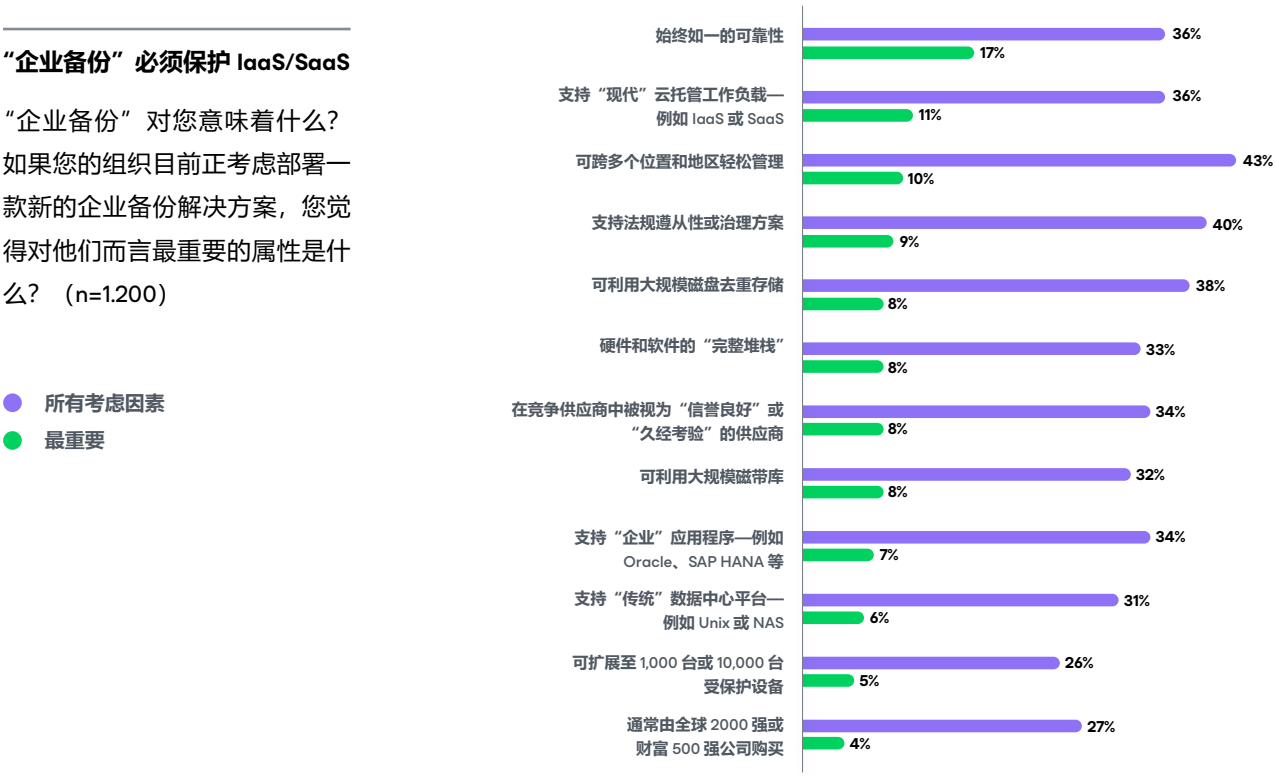
- **负责向组织交付 IT 的高管**
- **利用云服务的 IT 架构实施者**
- **负责内部和异地公司资源数据保护的备份专业人员**

“企业”备份必须保护 IaaS/SaaS

对 1200 家企业组织开展的调查显示，下一个数据保护解决方案最重要的两个功能是“提高可靠性”和“提高对云托管工作负载的保护”。

“企业备份”必须保护 IaaS/SaaS

“企业备份”对您意味着什么？如果您的组织目前正考虑部署一款新的企业备份解决方案，您觉得对他们而言最重要的属性是什么？（n=1,200）



虽然“企业”应用（例如 Oracle）和“传统”数据中心平台（例如 NAS）的保护仍然出现在更广泛的列表中，但两者的优先级都低得多，这可能是因为组织已经为这些传统平台部署了传统备份解决方案。相反，如果试图用传统备份方法来保护现代工作负载（如云），那么保护和恢复的可靠性在逻辑上就会大大降低。因此，将“可靠性”和“云保护”作为最重要的变革驱动因素也就不足为奇了。

对于 IT 领导者来说，有机会利用云托管基础架构来替代数据中心组件，应能提高运营灵活性和经济效益，因为可以在每个工作负载最理想的平台上提供 IT 服务。

对于混合架构师而言，当他们的团队对生产策略进行现代化改造时，必须注意同时对保护策略进行现代化改造，以免关键业务工作负载从数据中心内“保护良好”变为云中的“保护不足或无保护”。

对于数据保护专家来说，面临的挑战是利用云提供的各种实用程序（例如，每个生产云都提供复制作业、回收站或内置快照）来完善以数据中心为中心的标准备份解决方案，或者选择一个不仅能够保护传统工作负载，而且能够保护主流云的现代备份平台。后者还需提供一致性，因为工作负载可根据不断变化的业务需求在云之间流畅迁移。

现代保护必须不只是保护网络弹性

虽然数据保护现代化最明显的推动力应该是向网络弹性看齐，以应对无处不在、几乎不可避免的勒索软件威胁，但数据保护战略仅仅建立在这一迫在眉睫的威胁上，那将是大错特错。最新研究显示，虽然网络攻击是导致 IT 中断的最常见和影响最大的原因（40% 的组织遭受了攻击），但一直影响 IT 和业务流程的大多数其他危机仍然存在，包括：

37%
因**基础架构**问题而遭受中断

34%
由于应用程序软件**问题而**遭受中断

33%
因**人为错误**（如删除、覆盖等）而遭受中断

32%
由于操作系统**问题而**遭受中断

31%
因**公共云不可用而遭受中断**

29%
因**自然事件**（如火灾、洪水、恶劣天气等）**而遭受中断**

值得注意的是，在这些中断原因中，几乎没有哪个是因为利用云资源而不是自己的数据中心而得到缓解的。因此，云托管工作负载不仅对备份而且对灾难恢复有着相同的要求。虽然云服务可减少物理存储或服务器组件造成的错误，但使用现代数据保护方法保护数据中心的所有其他理由也应适用于混合云和公共云。

对于包括首席信息官和首席信息安全官在内的 IT 领导者而言，组织的灾难恢复策略本来就包含严重的 IT 中断事件，但现在必须扩大到包括网络攻击和公有云访问问题，并将其作为“准备工作”的一部分 。

对于混合架构师（包括 IT 架构师和具有安全意识的工程师）来说，提供云托管服务所需的专业模糊不同于访问控制和预防 / 检测安全专家与 IT 运营和 / 或基础设施、虚拟化、服务器等方面的专家的专业角色。虽然这种模糊性可能会让用户更加无缝地使用 IT 服务，但保护这些资源免受上述各种中断原因影响的负担更为艰巨。

对于数据保护专家来说，无论数据是由服务器还是服务提供的，数据就是数据，都必须采取普遍适用的数据保护方法。在这种情况下，“保护对象”现在必须包括云托管基础架构 (IaaS)、云托管文件和数据库等平台以及主流 SaaS 应用程序。

组织正在寻求“多云”的现代数据保护

当被问及“现代”数据保护最重要的方面是什么时，许多组织都提到了至少一项以云为中心的功能：

39%
希望能够在一个主要云之间迁移至另一个主要云（例如，从 Amazon 迁移到 Azure）

38%
希望对内部部署和 IaaS/SaaS 工作负载提供一致的保护

37%
希望其数据保护解决方案能够将内部部署工作负载迁移到云端

27%
希望将云基础架构用作灾难恢复站点

其中一些功能特别符合更广泛的 IT 需求：

对于 IT 领导者来说，所有这四种能力都能满足所希望的灵活性，以便组织选择是否利用云以及利用哪种云为业务对象提供 IT 服务。当组织为在数据中心内使用哪种虚拟机管理程序以及与哪种云进行互补而苦恼时，最热门的入侵方法无疑是最重要的。虽然几乎每个主要平台都提供将工作负载迁移到其技术的实用程序，但很少有（如果有的话）提供将其移动到其他地方的实用程序。因此，不出所料，IT 领导者对这项能力在现代数据保护方面给予了最高评价。

对于混合架构师来说，他们团队已经放弃无数个周末，将工作负载从服务器迁移到虚拟机管理程序，再迁移到替代虚拟机管理程序，现在又迁移到云端，但第一步始终都是做好备份，然后进行成功的测试还原。在今年的调查中，有理由认为 IT 实施人员会认识到，只需将备份“还原”到新云（又称迁移）即可。不仅备份经过“测试”，而且在迁移中止的情况下原始环境不会受到影响。

对于数据保护专家来说，在混合架构师公认的优势基础上，负责管理数据保护和利用上述功能的人员在现实中确实需要组织的数据保护解决方案能够同样保护多元数据中心和主流云服务，并将在虚拟机管理程序或云上受到保护的服务器实例“转换”为将该服务器实例还原到不同的虚拟机管理程序或云主机时所需的结构。例如，将 Amazon 备份到 Azure、将 VMware 备份到 Hyper-V、将 VMware 备份到 Azure 等 ...

这些考虑因素如何推动变革

鉴于采用“云智能”战略可以带来如此潜在的敏捷性和有效性，利用混合云和多云战略的热情理所当然地高涨。但是，如果没有一套专为现代企业的无数云环境构建的现代数据保护功能，许多数字化转型和 IT 现代化的努力都将落空。因此，也就难怪 92% 的组织增加了 2024 年的数据保护预算，平均增幅为 6.6%，而 IDC 的总体 IT 预算增幅预测仅为 3.5%。换句话说，虽然 IT 部门的总体预算可能略高，但不成比例的数据保护投资增加可能会以牺牲其他优先级较低的 IT 计划为代价。

对于可能推动预算规划的 IT 领导者来说，这表明他们致力于确保数据中心和云中的所有数据都得到保护。

对于混合架构师而言，“生产现代化的同时，保护也必须现代化”，这是对整体数据保护需求的保证和认可。

对于负责实现这些成果的数据保护专家来说，54% 的组织打算在 2024 年期间更换其主要备份解决方案，这一点不足为奇。虽然有些组织可能会使用另一种能够保护各种云的主流备份来补充其传统的数据中心备份解决方案，但这可能会成为催化剂，使传统备份解决方案的“变革压力”被“为每个独特的云服务运行多个点产品所带来的压力”所轻松抵消。

本研究简报基于 1200 份调查反馈，这些反馈来自负责组织数据保护策略的公正 IT 领导者和实施者，调查于 2023 年底进行，并于 2024 年 1 月发布。数据由 ESG 和 Gartner 的前分析师整理和撰写，他们在数据保护行业共计拥有 70 年的经验。

如需下载完整的《2024 年数据保护趋势报告》，请点击此处

Jason Buffington
@JBuff
市场战略副总裁
Veeam Software

戴夫 · 拉塞尔
@BackupDave
企业战略副总裁
Veeam Software

关于 Veeam Software

作为数据保护和勒索软件恢复领域首屈一指的全球市场领导者，Veeam 的使命是帮助每个组织通过混合云的数据安全、数据恢复和数据自由实现极致弹性。Veeam Data Platform 可确保其应用和数据受到保护并始终可用，让 IT 和安全领导者高枕无忧。Veeam 总部位于西雅图，在 30 多个国家 / 地区设有办事处，为全球 450,000 多家客户提供保护，这些客户信赖 Veeam 以确保其业务正常运行。极致弹性始于 Veeam。请访问 www.veeam.com 了解更多信息或关注 Veeam 的 LinkedIn @veeam-software 和 X @veeam。