在混合云环境中部署统一安全

复杂的分布式资源要求企业实现统一且简化的混合云安全

假如保障云端的安全能够加速企业的业务增长，会怎么样呢?

似乎每个人都了解云。为了实现性能、可靠性和成本节约方面的目标，越来越多的企业采用云来提高软件的可靠性和可扩展性。通过迁移至云端，企业减少了维护物理服务器及其相关网络基础架构的需求；但是，值得注意的是，在云环境中，企业的安全责任不会减轻，相反，他们需要承担保护云端和本地部署的数据与工作负载的责任。

尽管云服务提供商(CSP) 可能提供了某种级别的安全性，混合云架构仍然很复杂，需要企业安全团队的持续管理，才能确保数据和工作负载安全无虞。

如今，合规性要求越来越多，比如《通用数据保护条例》(GDPR)， 高级威胁也越来越多，以及需要和业务同步前进的要求，安全团队需要提供一个全面的安全框架来保护云环境和本地部署环境。

将安全放在首位，这是构建混合云安全框架的关键一步。如果能够实现设计安全，并从一开始就将安全控制植入 DevOps 流程和云迁移计划，那么贵企业不需要投入宝贵的时间和资源来被动应对威胁与合规性问题，也就是说，安全能够加速企业的业务增长。

向云和混合云环境迁移后，本地部署和云系统管理员所承担的责任也发生了变化。

IBM Security 的混合云保护方法

尽管云能够在某种程度上抵御零日漏洞攻击和内部攻击，但是单靠云并不能提供企业期望和需要的企业安全控制方法来使用云服务。2017 年的一项调研表明，42% 的受访企业表示他们的混合云环境遭受了攻击。[1] 另一项调研则表明，超过一半的受访企业（其中包括多家医疗保健机构）有非常容易修复的网络漏洞，如使用过时的浏览器和陈旧的或未更新补丁的操作系统。[2]

与本地部署的 IT 环境一样，混合云环境也存在类似的安全问题和要求，比如保护数据、保障系统，确保监管合规性。但是，混合云环境还面临另外一个挑战，即，以同样的速度保护云环境和本地部署环境中的数据，并给予同样的关注。

IBM Security 的混合云保护方法能够满足关键的企业级安全需求，并且专注于保护数据、提高生产力，以及确保合规性。

保护数据

数据是委托给企业或者由企业创造的最宝贵、最重要的资产之一。在混合云环境内，云同时存储在本地部署和云端，并且在数据存储点、端点和设备访问点之间移动。针对混合云环境，您需要用您自己的安全控制方法来补充云服务提供商的安全方法，确保您的数据安全无虞。

提升生产效率

对于任何企业来说，用于生产的时间和资源都是企业成功的关键。因此，如果花费时间和资源来处理本来可以预防的安全事故，企业可能就无法高效地持续实现业务增长。通过与 DevOps 团队密切合作，以提供安全框架和必要的工具，从一开始就植入安全控制方法，那么企业就不需要将来回退以增加安全控制，生产力也就不会受到影响。

确保合规性

实现和维持合规性是一项复杂的任务，尤其是在混合云环境中，因为异构环境中存在独特的合规性挑战。因此，为了在混合云环境中实现并维持合规性，企业需要可见性和报告，既包括云系统，也包括本地部署系统，这一点至为关键。

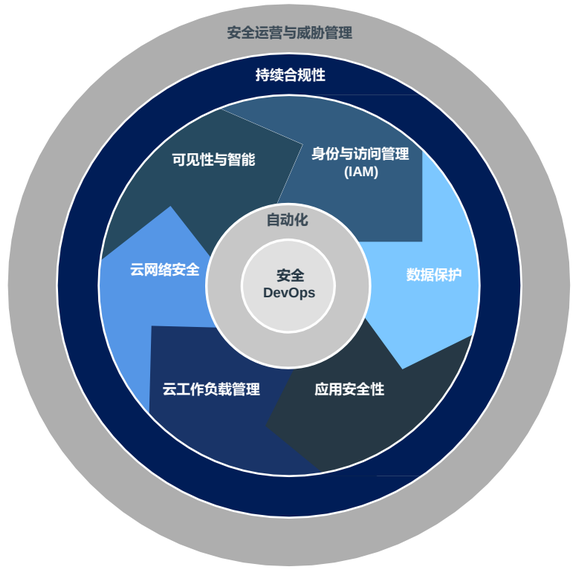
1 “Zero-Day Exploits Are Most Prevalent Attack in Hybrid Cloud Environments”. 来自 Capsule8 赞助的调研. *Capsule8.* 2018 年 2 月 28 日.

2 Heather Landi. “Report:15 Percent of Healthcare Organizations Running Outdated Operating Systems”. *Healthcare Informatics*. 2017 年 6 月 8 日.

IBM Security：关注领域和功能

为了详细剖析您需要哪些元素才能确保云环境和内部环境的安全性，圆盘图提供了十个关注领域和功能，用于构建全面的安全框架。

点击圆盘了解更多信息 →

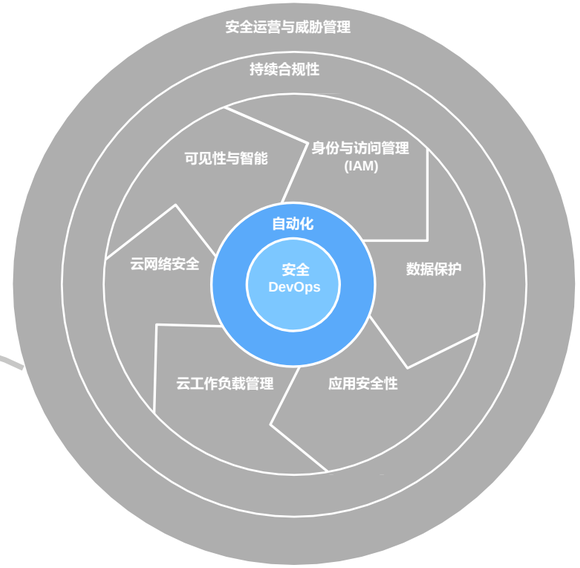


安全 DevOps

一切都从关注 Secure DevOps 开始。业务线主管向 DevOps 团队施加压力，要求他们迅速且大规模地实现云计划的价值。这些团队需要得到安全策略和架构的支持，以便在云端开发应用和工作负载，并且从一开始就将安全铭记于心，而非之后再补救。

自动化

通过将自动化的安全策略、安全技术和漏洞扫描配置集成至混合云环境和工作负载中，您能够避免将宝贵的时间和资源用在被动应对威胁上。

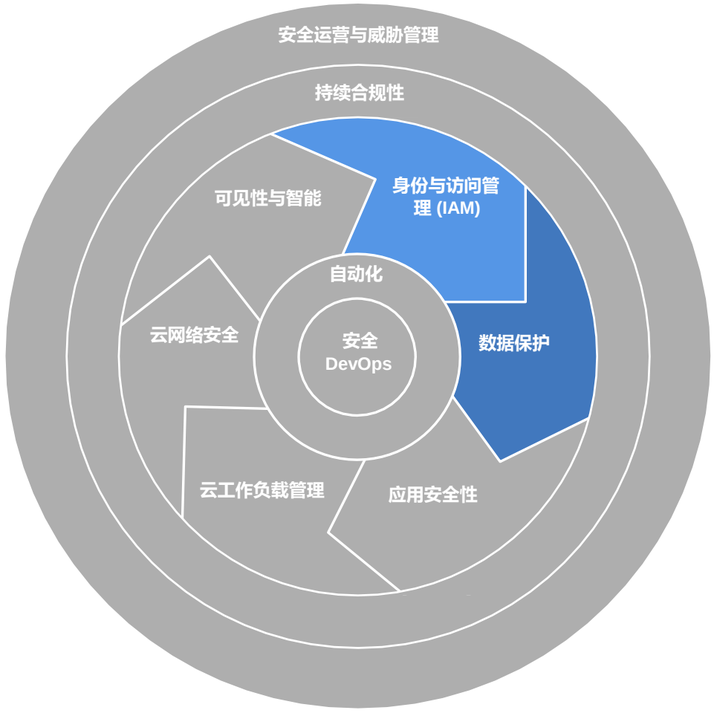


身份与访问管理 (IAM)

混合云架构本身会使得攻击者可能窃取宝贵数据的位置大幅增加。安全软件如果能覆盖多个系统，管理员就能采用统一的身份和访问策略，查看访问日志和其他记录，同时交付无缝的用户体验。

数据保护

在混合云环境中，安全组件必须在多个系统保持一致，这样才能保护数据免于遭受内外部威胁。保护本地部署边界以内和以外的数据（包括跨多个云平台的数据）。



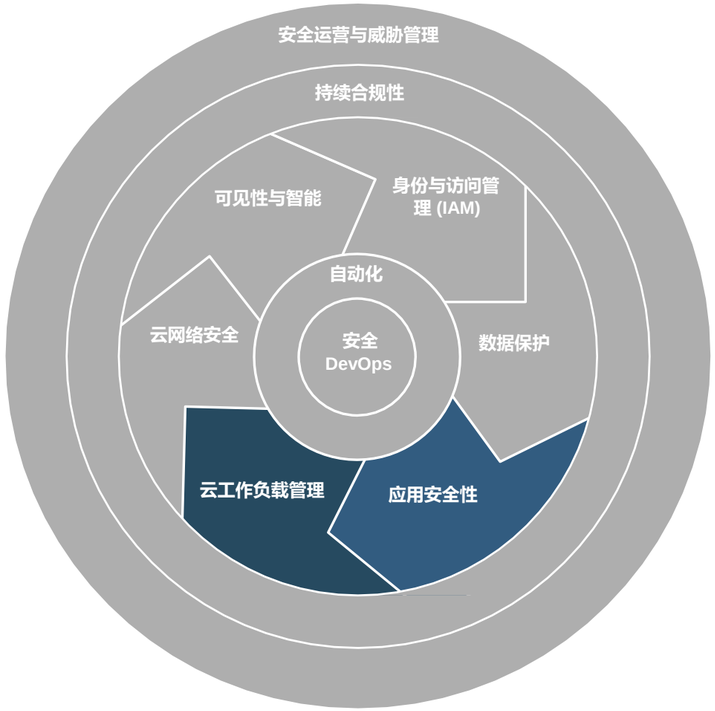
点击圆盘了解更多信息

应用安全性

应用的未来在于以云为基础。为了将企业安全的价值最大化，开发人员需要在应用上线之前，利用工具自动消除应用安全风险，并智能地报告代码中的漏洞。在开源组件方面，云的安全性取决于自动化安全测试，用以评估采用的代码。

云工作负载管理

管理员仅有有限的时间来处理混合环境中的安全问题。鉴于资源有限，他们必须确定问题的优先级。归根结底，企业必须大规模采用满足以下要求的安全软件和服务解决方案：能够利用自动化技术，在混合云生态系统中高效扫描漏洞，并应用策略和安全修复。



点击圆盘了解更多信息

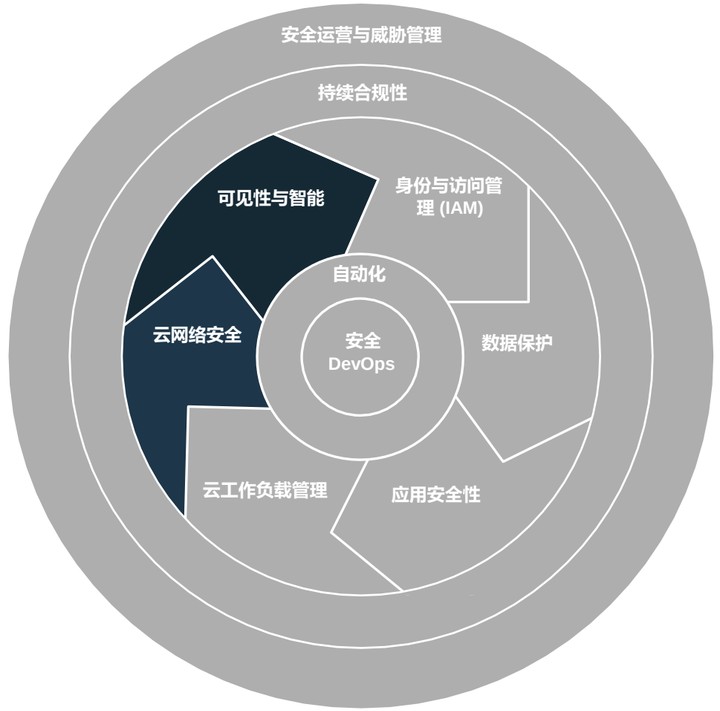
攻击者依赖困扰安全管理员的疏忽和滞后。为了有效保护混合云系统，企业需要高度重视整合且最新的日志和其他安全数据视图，这样，IT 人员和安全分析师就能快速发现异常情况，并针对每家云服务供应商（CSP ）采用一致的方法应对这些异常。

可见性与智能

混合云环境可能多种多样，十分复杂。因此，您必须掌握企业内的威胁和漏洞，确保快速、准确地应对各类安全事故。

云网络安全

因为云系统可能极具挑战性，所以保护云系统需要灵活性、速度、自动化，以及与本地部署系统保持一致。理想的系统应该确保应用能够跨越多个 CSP 云环境和本地部署系统安全运行。



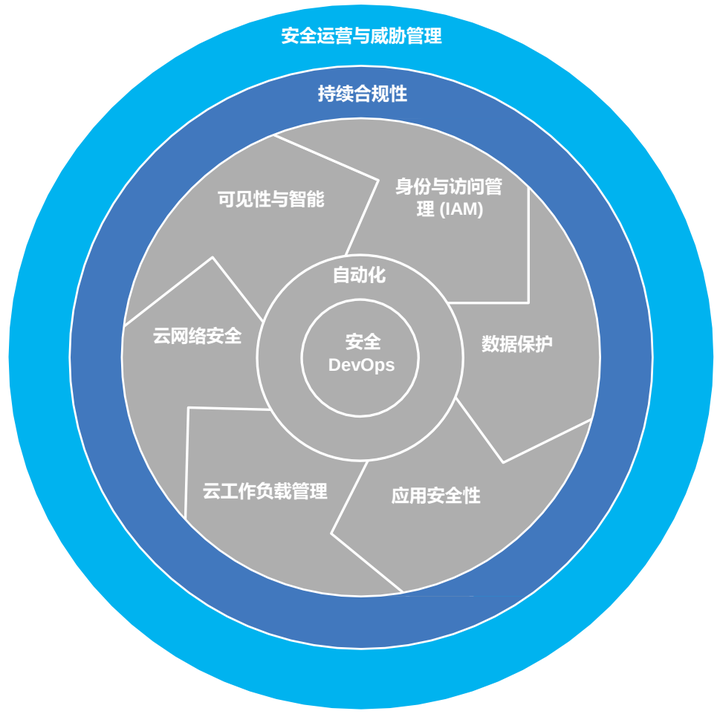
点击圆盘了解更多信息

安全运营与威胁管理

要实现有效的安全运营与威胁管理，您需要通过单一且统一的安全框架，跨越本地部署工作负载和云工作负载实现集中管理和可见性。您的安全运营中心（SOC）和团队将需要继续检测已知和未知的威胁，超越个别警报的处理，识别潜在的事故并确定优先次序，并应用 AI 加速调查过程。

持续合规性

对于大多数组织而言，尤其是对于 DevOps 团队，实现并持续满足监管法规、行业法规的合规要求是一项非常艰巨的任务。贵企业可以利用基于AI的软件提前确保合规性，并持续跟进监管趋势；利用动态监控工具，跟踪整个企业的合规性风险；利用自动化技术，简化审计和报告；利用服务，交付宝贵的专业知识和洞察力。



点击圆盘了解更多信息

IBM 的混合云安全解决方案

不论贵企业在云领域中位于何处，IBM 的产品和服务都能通过一个全面的混合云安全框架，提供所需的关注领域和功能。

领先的 IBM Security 产品

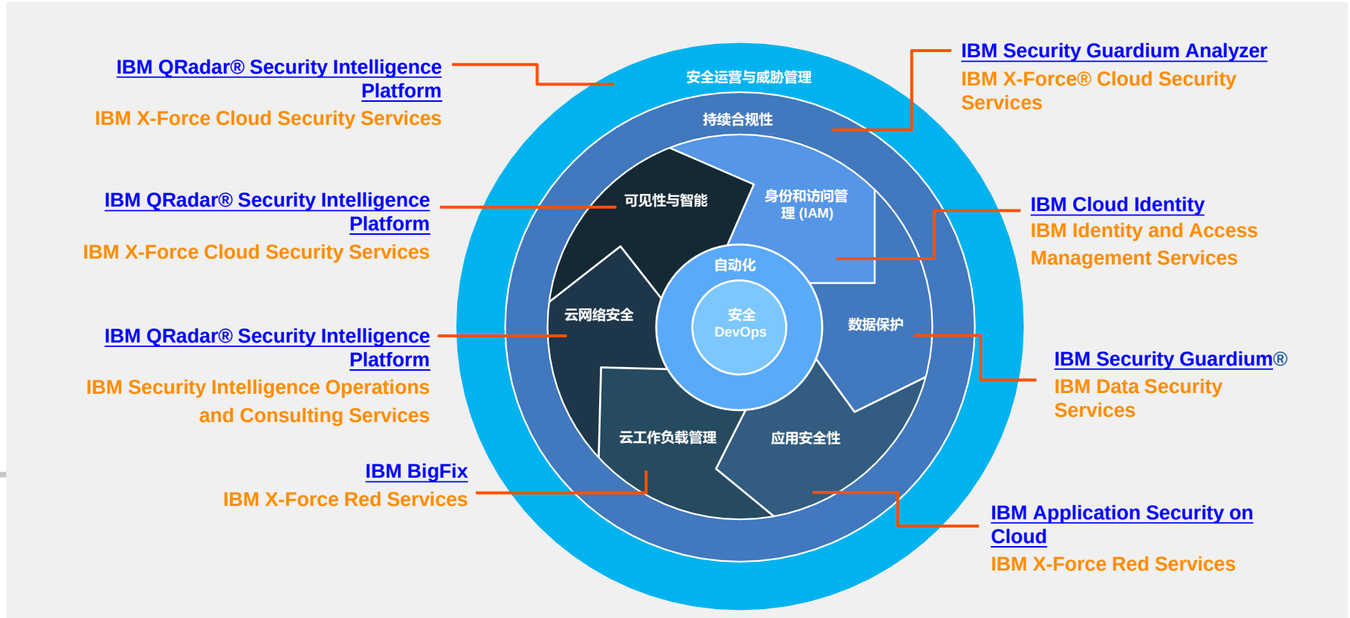
– IBM Security Guardium®
- IBM Security Guardium Analyzer
- IBM Application Security on Cloud
- IBM Cloud Identity
- IBM QRadar® Security Intelligence Platform

– IBM BigFix

专家级 IBM Security 服务

- IBM X-Force® Cloud Security Services
- IBM Data Security Services
- IBM Identity and Access Management Services

– IBM X-Force Red Services
- IBM Security Intelligence Operations and Consulting Services



有关更多信息

如欲了解有关混合云安全的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：**ibm.com**/security

关于 IBM Security 解决方案

IBM Security 可以提供最先进、集成的企业安全软件和服务组合。由世界知名的 IBM X-Force 研发团队提供支持的这一产品组合可提供一流的安全智能，帮助企业全面保护其人员、基础架构、数据和应用，进而提供身份与访问管理、数据库安全、应用开发、风险管理、终端设备管理、网络安全等解决方案。这些解决方案可以帮助企业有效管理风险，为移动、云、社交媒体和其他企业业务架构落实集成安全。IBM 作为世界上覆盖范围最广的安全研究、开发和交付企业之一，每月对 130 多个国家/地区的超过 1 万亿个安全事件进行监控，并拥有 3,000 多项安全专利。

此外，IBM 全球融资部可提供各种支付选项，进而帮助您获取开发业务所需的技术。我们可提供 IT 产品和服务的全生命周期管理（从收购到处置）。有关更多信息，敬请访问：**ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

美国印刷
2019 年 3 月

54015454-CNZH-01