云平台安全指南

IBM

要点

1 理想状态下，云提供商应能将您的身份管理系统集成到他们的平台中，而且在任何情况下，均应为您提供一个可信的身份管理解决方案，以供您在需要时使用。

2 作为建立信任过程的一部分，验证并确保云平台能够提供良好集成的防火墙和安全组，还可基于工作负载和可信的计算主机提供微分段选项。

3 要求云提供商提供 BYOK 解决方案，使您的组织能够专门管理所有数据存储和服务中的密钥。

4 面向容器的最佳安全实践是在部署之前和运行过程中均进行漏洞扫描。

5 云平台的安全机制必须要高效控制访问，在工作负载级别上运行，跟踪活动详情并集成到内部系统之中。

重新思考云应用的安全

随着越来越多的组织转而采用针对应用开发和工作负载管理的云原生模型，云计算平台正在快速限制着基于边界的传统安全模式的有效性。尽管边界安全机制依然很有必要，但就其本身而言，并无法完全确保安全。由于云端的数据和应用都处在旧的企业边界之外，因此必须采用新方式对这些数据和应用加以保护。

对于正在转变到云原生模式或计划采用混合云应用部署的组织而言，必须通过有助于保护云工作负载安全性的技术来补充传统的基于边界的网络安全机制。企业必须确保云服务提供商能够保证从基础架构起往上的整个堆栈的安全。因此，在选择提供商时，基本的一点就是要建立对平台安全性的信任。

云安全的驱动因素

数据保护和监管合规性都是云安全的主要驱动因素，同时它们也是云采用的妨碍因素。这些问题的解决涉及到开发和运营的各个方面。在云原生应用中，数据可能分布在各个对象存储、数据服务和云平台之中，这就为潜在攻击提供了多个攻击面。此外，攻击并不仅仅来自于技术纯熟的网络黑客和外部来源；近期的一项调研结果显示，53% 的受访者表示他们在之前 12 个月内曾遭遇过内部人员攻击。[1]

云安全的五大基础要点

组织若要解决云平台使用方面的特定安全需求，就需要确保他们的提供商成为可信赖的技术合作伙伴。事实上，组织应根据这五个安全方面评估云提供商，因为它们与组织自身特定需求有关：

1. 身份与访问管理：认证、身份和访问控制
2. 网络安全：保护、隔离和分段
3. 数据保护：数据加密和密钥管理
4. 应用安全和 DevSecOps：包括安全测试和容器安全
5. 可视性与智能：监控并分析日志、工作流和事件，以从中发现模式

在云平台上验证身份、管理访问

与云平台的任何交互都是从身份验证开始的，即确定谁在进行交互，这种身份可以是管理员或是用户，甚至可以是某个服务。在 API 经济中，服务都有其身份，因此能够准确地、安全地基于身份对服务进行 API 调用对于成功运行云原生应用至关重要。

因此，应选择能够对 API 访问和服务调用提供统一身份认证方式的提供商。此外，您还需要一种能够对访问云端托管应用的最终用户进行识别和认证的方式。举例来说，IBM® Cloud 采用了"应用 ID (App ID)"方式，支持开发人员将认证组件集成到移动和 Web 应用中。

强大的认证机制有助于防止非授权用户访问云系统。由于平台身份与访问管理（IAM）如此重要，因此，拥有现有系统的组织应确保云提供商能够集成企业的身份管理系统。这一点通常通过身份联合技术来实现，即实现每个用户的 ID 与属性的跨系统关联。

为何要认证服务调用？

在基于微服务的架构中，API 能够让应用相互之间进行通信、共享数据。当某个应用在运行时，它会使用 API 调用服务，以完成各种操作。举例来说，您的应用可能会调用数据对象存储服务。为了执行该请求，该对象存储服务本身可能会调用密钥管理服务，以获得解密数据所需的加密密钥。作为用户体验交付的一部分，应用可能会使用 API 访问用户身份信息，在应用之间传递内容（比如将内容从应用传递到 Twitter）并确定用户的位置，以便提供位置特定的信息。所有这些集成点都会带来安全挑战。

云提供商应采用统一的方式来认证需要访问某个 API 或服务的用户或服务的身份。当然，作为认证流程的一部分，所有的访问请求会话和事务处理均应予以记录，以供审计使用。API 和服务很有可能都拥有宝贵的知识产权；您不会希望任何人都能使用。

要求潜在的云提供商证明他们的 IAM 架构和系统涵盖了所有基本要点。举例来说，IBM Cloud 的身份和访问管理基于多个关键功能（图 1）：

身份

- 每个用户都有一个唯一标识
- 服务和应用通过它们的服务 ID 进行识别
- 资源由云资源名称 (CRN) 进行识别和处理
- 用户和服务通过他们的身份进行认证并发放令牌

访问管理

- 当用户和服务尝试访问资源时，IAM 系统会确定是否允许此类访问和操作
- 由服务来定义操作、资源和角色
- 由管理员来定义分配用户角色及各种资源访问权限所依据的策略
- 将保护扩展到 API、云功能及托管在云端的后台资源

在您评估云提供商的安全功能时，应查看访问控制表及公共资源名称，这些内容支持您对用户施加限制，不仅是限制其只能访问特定资源，还能限制其只能对这些资源执行特定操作。这些功能有助于保护您的数据免于遭受来自外部和内部的非授权访问。

在您基于使用企业身份提供商 (Enterprise IdP) 的现有企业应用构建云原生应用时，将您的 Enterprise IdP 扩展到云端尤为有用。您的用户无需使用多个系统或 ID，便可通畅地登录到云原生应用和基础性应用。因此说，降低复杂性始终都是一个非常重要的目标。

要点

理想状态下，云提供商应能将您的身份管理系统集成到他们的平台中，而且在任何情况下，均应为您提供一个可信的身份管理解决方案，以供您在需要时使用。

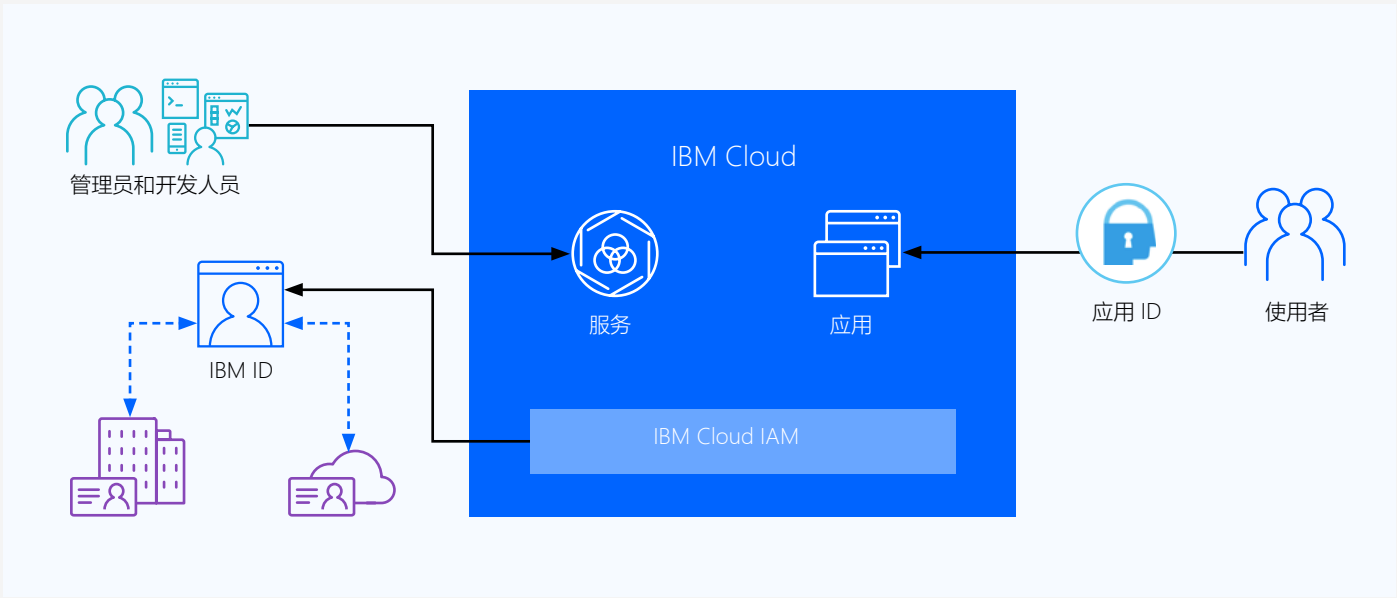

图 1：由提供商管理的集群元素与由客户管理的集群元素之间的分离。

重新定义网络隔离与保护

许多云提供商都使用网络分段来限制对同一网络中的设备和服务器的访问。此外，提供商还会在物理基础架构的基础上构建虚拟的独立网络，并自动将用户或服务限制到特定独立网络。这些技术连同其他的基本网络安全技术都是确立云平台可信赖性的“筹码”。

云提供商会以软件定义网络安全服务的形式提供各种保护技术，包括 Web 应用防火墙、虚拟私有网络和服务拒绝减缓等，并按照使用量收费。在云计算时代，您可以考虑采用以下技术作为关键网络安全组件。

安全组和防火墙

云客户通常会采用网络防火墙来进行边界保护（虚拟私有云/子网级网络访问），并针对实例级的访问构建网络安全组。安全组是云资源的访问授权的“第一道防线”。借助这些安全组，您可以轻松地添加实例级的网络安全组件，以管理公有网络和私有网络上的入站和出站流量。

许多客户都需要边界控制组件来确保边界网络和子网的安全，而虚拟防火墙可以满足这一要求，而且可轻松完成部署。防火墙的作用是防范非预期的流量进入服务器、减少攻击面。因此，您需要确保云提供商能够同时提供虚拟防火墙和硬件防火墙，使您能够为整个网络或子网配置基于授权的规则。

当然，VPN 可为您提供从云返回到内部资源的安全连接。如果您运行的是混合云环境，就必须采用 VPN。

微分段

以小型服务集的形式开发云原生应用能够实现一定的安全优势，这有助于您使用网络分段将其隔离开来。因此，您需要一个能够通过网络配置和供应自动化来实施微分段的云平台。基于微服务模型而构建的容器化应用正在快速成为可扩展的工作负载隔离支持方面的常态方法。

要点

作为建立信任过程的一部分，验证并确保云平台能够提供良好集成的防火墙和安全组，还可基于工作负载和可信的计算主机提供微分段选项。

通过加密和密钥管理保护数据

可靠的数据保护是任何数字企业的安全基础，尤其是在金融服务和医疗等高度监管行业。

与云原生应用相关的数据可能分散在多个对象存储、数据服务和云平台之中。传统的应用可能拥有它们自己的数据库和 VM，并在文件中存储它们的敏感数据。在这些情况下，无论是动态数据还是静态数据，敏感数据的加密都非常关键。

企业都非常担心云运营商或其他非授权用户在他们不知情的情况下访问他们的数据，而且也希望实现数据访问的完全可视性。通过加密来控制数据访问并控制对加密密钥的访问已成为众所期望的安全功能。如此一来，自带密钥 (BYOK) 模式已成为当前的云安全需求之一。通过该模式，您可以在一个集中位置管理加密密钥，确保根密钥不会脱离密钥管理系统的边界，使您可以审计密钥管理生命周期内的所有活动（图 2）。

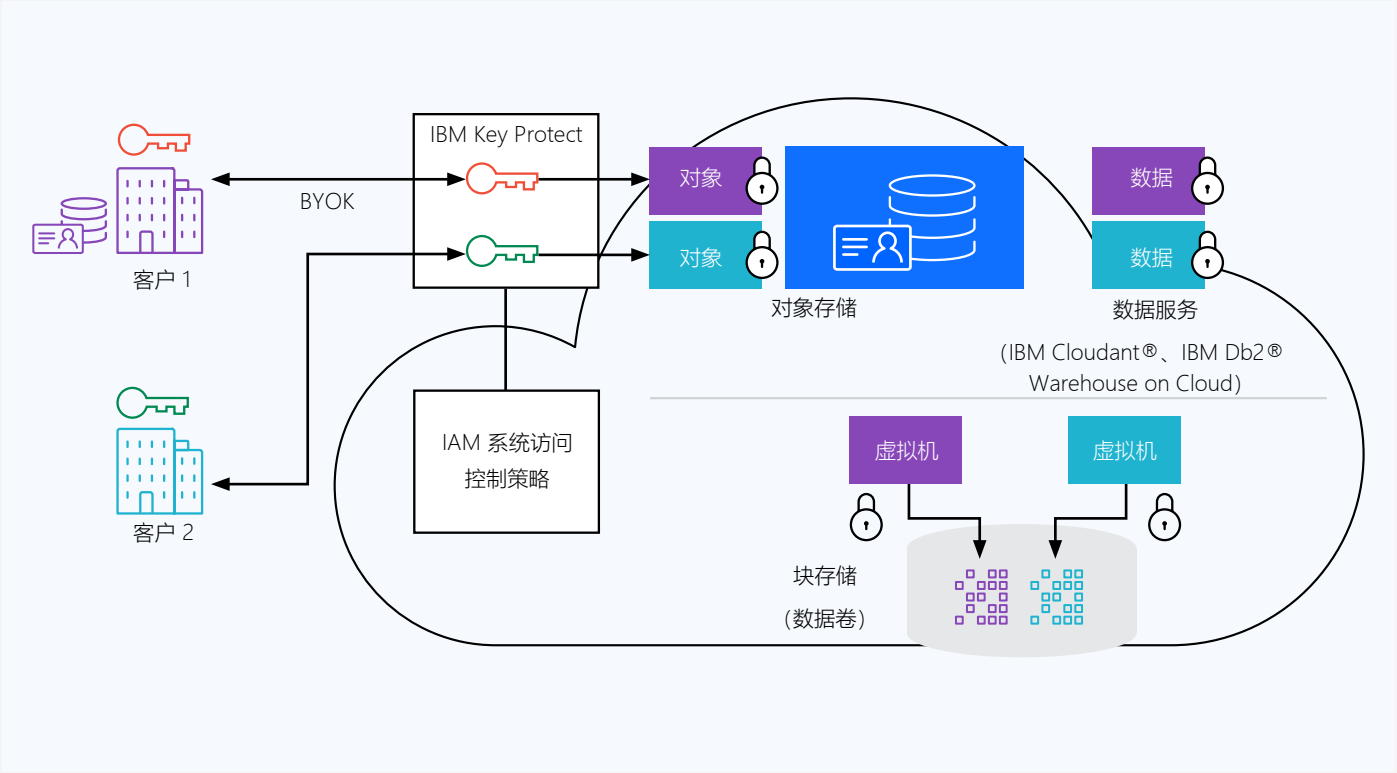

图 2：BYOK 解决方案的架构。

可信的计算主机

我们再来谈谈硬件：任何企业都不希望将宝贵的数据和应用部署在不可信的主机上。云平台提供商如果在硬件方面采用"测量-验证-启动"协议，就能够为您提供高度安全的主机，便于您在容器编排系统内部署应用。

举例来说，Intel 的可信执行技术 (Intel TXT) 和可信平台模块 (TPM) 都属于可确保云平台可信赖性的主机级技术。Intel TXT 能够防范基于软件的攻击，这些攻击的目的是通过破坏系统或 BIOS 代码或修改平台配置的方式盗取敏感信息。Intel TPM 是一款基于硬件的安全设备，可确保在向操作系统发布系统控件之前，操作系统不会被篡改，以此方式确保系统启动进程的安全。

静态数据和动态数据保护

借助基于 BYOK 的内置加密机制，无论数据是位于内部还是位于云端，您都可以维持数据的可控性。对于云原生应用部署环境中的数据而言，这是进行数据访问控制的一种绝佳方法。在该方法中，客户的密钥管理系统会在内部系统中生成一个密钥，然后将其传输到提供商的密钥管理服务中。这种方法在块存储、对象存储和数据服务存储等各种存储类型中，都采用的是静态数据加密。

对于动态数据而言，则是通过传输层安全性/安全套接字层 (TLS/SSL) 确保安全的数据通信和传输。TLS/SSL 加密还可帮助您确保实现合规性、安全性和治理要求，无需对密码系统或基础架构进行管理控制。因此说，若要确保云平台的可信赖性，SSL 证书的管理能力也是必需的要求之一。

满足审计与合规要求

提供您自己的加密密钥并将其保存在云端（并确保服务提供商无法访问），便可实现 CISO 合规性审计所需的信息可视性与可控性。

要点

要求云提供商提供 BYOK 解决方案，使您的组织能够管理所有数据存储和服务中的密钥。

实现 DevOps 安全自动化

在 DevOps 团队构建云原生服务并采用容器技术时，他们需要借助一种高效的方式，将安全检查控件集成到日益自动化的管道之中。由于 Docker 中心 (Docker Hub) 等站点都鼓励开放交换，因此开发人员只需下载他们所需的资源即可，这样便可节省映像准备时间。不过，在确保这种灵活性的情况下，就需要在部署注册表中的所有容器映像之前，对它们进行例行检查。

借助自动化的扫描系统，您可以在运行映像之前搜索它们之中的潜在漏洞。因此，您应询问平台供应商，作为 DevOps 管道安全的一部分，他们是否允许您的组织创建策略（例如："不得部署有漏洞的映像"或"在将这些映像部署到生产环境之前提醒我"）。

举例来说，IBM Cloud Container Service 提供了一个"漏洞顾问"（Vulnerability Advisor，VA）系统，该系统可实现静态/动态容器扫描。在部署映像之前，VA 会检查云客户私有注册表中每个映像的各个层，以检测其中是否存在漏洞或恶意软件。仅仅简单地扫描注册表中的映像会遗漏一些问题，比如静态映像会缓慢移动到已部署的容器之中；为此，VA 还会对运行中的容器进行扫描，以检测其中是否存在异常。此外，它还会以分层式警报的形式提供相关建议。

要点

面向容器的最佳安全实践是在部署之前和运行过程中均进行漏洞扫描。

VA 中有助于实现 DevOps 管道安全自动化的其他功能包括：

- 策略违例设置：借助 VA，管理员可以基于下述三种映像故障情形设置映像部署策略：安装了带有已知漏洞的软件包；启用了远程登录；有些启用远程登录的用户使用了容易猜到的密码。
- 最佳实践：VA 目前会按照 ISO 27000 检查 26 种规则，包括密码最短使用期限、密码最小长度等设置。
- 安全误配置检测：VA 会标记每个误配置问题并提供相关描述，同时还会推荐相应的补救措施。
- 与 IBM X-Force® 相集成：VA 融合了来自 5 个第三方来源的安全智能，并采用了攻击向量、已知修复包的复杂性和可用性等标准来评定每个漏洞。评级系统（采用"关键"、"高"、"中等"或"低"等级别）有助于管理员快速了解漏洞的严重性并确定补救的优先级。

在补救方面，VA 在修复时不会中断正在运行的映像。相反，IBM 会恢复注册表中的"黄金"映像，并在容器中部署一个新映像。这种方法有助于确保该映像在未来的所有实例化都可以采用同一修复包。VM 仍旧可以使用传统方法处理：使用终端设备安全服务来安装 VM 补丁、修复 Linux 安全漏洞。

Kubernetes 相关

如果您的 DevOps 团队采用了 Kubernetes 容器统筹安排软件，则应确保它们可以继续使用相关的常用工具。此外，你还需评估平台在供应新的 Kubernetes 集群及管理现有 Kubernetes 集群方面的难易程度。

询问云平台提供商他们的 Kubernetes 系统是否支持 Calico 和 Istio。Calico 和 Istio 是 Kubernetes 的两个重要组件，有助于确保应用和工作负载的安全性。Calico 有助于简化分配到计算节点中工作负载的 IP 地址的管理，而且能够对每个计算节点中的访问控制列表进行编程，以执行安全策略。借助通过配置标签进行设置和执行的策略定义，Istio 可以采用基于证书的方式控制 Kubernetes pod 或集群中的微服务之间的通信。

通过智能监控构建安全免疫系统

在迁移到云端时，CISO 通常会担心可视性较低、可控性损失等问题。如果某个特定密钥被删除，或者由于某个无意的配置更改而导致需要重建与内部资源或企业安全运营中心（SOC）的连接，组织的整个云性能就会下降；因为这个原因，运营工程师必须要求云提供商确保对基于云的工作负载、API、微服务等的完全可视性。

访问痕迹和审计日志

由云提供商或您的组织进行的所有用户访问和管理访问均应自动予以记录。通过内置的云活动跟踪程序，可以跟踪对平台及服务的所有访问痕迹（包括 API、Web 和移动访问）。您的组织应能使用这些日志并将其集成到企业 SOC 之中。

企业安全智能

确保您可以选择性地将所有日志和事件集成到内部安全信息与事件管理（SIEM）系统之中（图 3）。一些云服务提供商还会提供安全监控及事件管理与报告功能、安全警报实时分析功能，以及混合部署的集成式视图。

举例来说，IBM QRadar® 是一款综合性的 SIEM 产品，它提供了一系列可随着组织的需求增长而不断扩展的安全智能解决方案。该产品的机器学习功能可以按照威胁模式进行训练，并以此方式构建预测性安全免疫系统。

具有专业知识的托管安全服务

如果您的组织不具备充分的安全专业知识，则可以选择能够帮助您管理安全的提供商。一些提供商能够监控您的安全事件，运用来自各个行业的威胁情报并关联此类信息，然后采取相应行动。您还应该询问提供商是否可以提供与内部/托管安全服务相集成的单个控制面板。

要点

云平台的安全机制必须要高效控制访问，在工作负载级别上运行，跟踪活动详情并集成到内部系统之中。

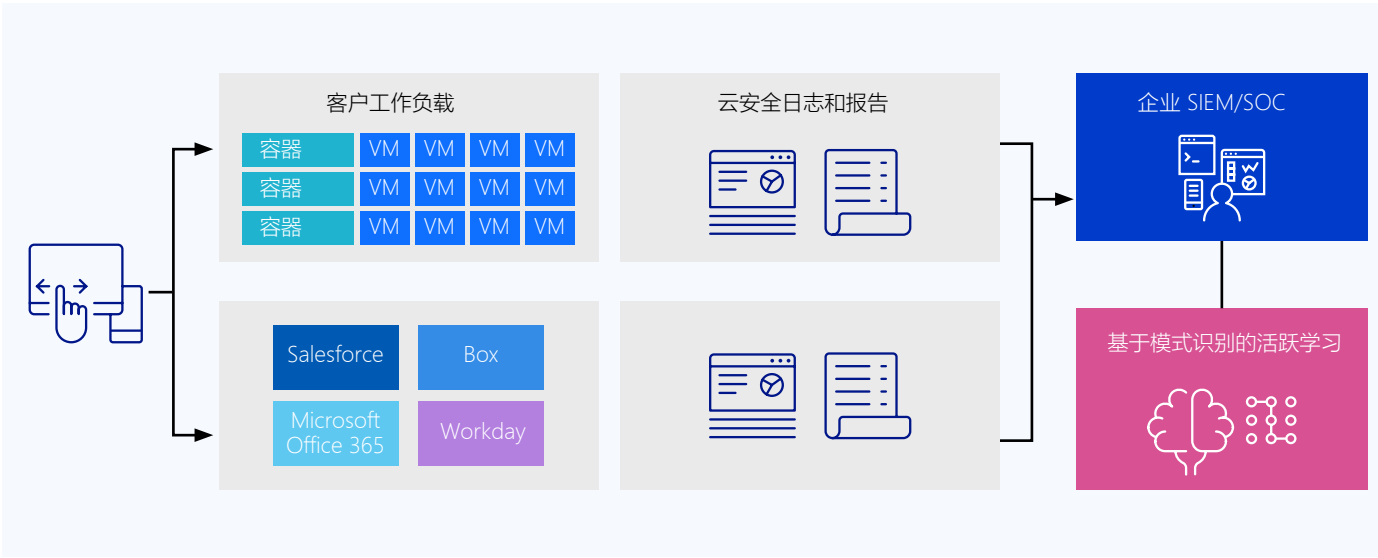

图 3：将云可视性集成到企业 SIEM/SOC 之中。

有助于实现业务成功的安全性

云技术已成为数字企业运营中占比越来越重也越来越重要的一部分，因此您应该选择那些能够提供适当的安全功能与控件集的供应商，帮助您高效保护您的数据、应用，以及面向客户的应用所依赖的云基础架构。因此，您要确保您所选的云平台安全解决方案能够覆盖下述五大关键云安全领域：身份与访问；网络安全；数据保护；应用安全；可视性与智能。我们的目的在于减少对技术的担忧，更多的专注于核心业务。

高度安全的云平台可帮助您实现显著的业务优势和 IT 优势，包括：

- 加速实现价值：由于安全组件已经安装并配置完毕，因此团队可以轻松地配备资源，快速完成用户体验的原型设计，评估结果并根据需要进行迭代。
- 降低资本开支：借助云端的安全服务，可以消除许多前期成本，包括服务器、软件、许可证和设备方面的成本。
- 减轻管理负担：通过成功建立并维持客户对云平台的信赖，拥有合适安全产品的云提供商就会承担大部分的管理负担，帮助您降低报告和资源维护方面的成本。

有关更多信息

有关云安全的五大关键领域以及 IBM 所提供的相关技术和服务的更多信息，敬请访问：ibm.com/cloud/security

保持在线

IBM Cloud 博客

关注我们

@IBMcloud

Facebook

联系我们

LinkedIn

YouTube

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

美国印刷
2018 年 1 月

[1] 2018 年内部人员威胁报告，发布于 2017 年 11 月。
http://crowdresearchpartners.com/portfolio/insider-threat-report