买家指南

# 哪个安全平台最适合您?

提出正确的问题。得到正确的答案。

IBM Security

IBM

# 选择正确的安全平台

为您的组织寻找安全平台可能是一项艰巨的任务。在网络安全领域，“平台”一词已被过度使用，导致企业难以消除“噪音”，也难以了解哪些因素在企业选择最佳业务选项时最为重要。您今天所选的平台可以作为未来几年安全成熟度的基础，因此应谨慎选择。

企业安全团队面临着数据和工具过多以及资源不足的挑战。就目前而言，我们需要采用另一种方式来统一安全数据、工具和团队，而且迫切需要将所有内容集中在单个位置，这便是集成式安全平台的好处。

## 您希望在安全平台中寻找什么功能

若要找到一个可在现在和未来均能确保高效性的整体集成式网络安全平台，您应考虑以下因素：

- 与数据移动相关的考虑事项
- 部署选项
- 您需要与其他工具的连接
- 平台的开放性与适应性
- 它支持的功能和服务

请考虑以下关键问题，以便您了解选择安全平台时的选项，并确定哪个选项最适合您的组织。

**1 您是否需要移动数据以便从中获取价值?**

许多安全平台需要将所有数据移动到该平台上才能访问这些数据。虽然将所有数据放在单个位置似乎是个好办法，但它可能会很复杂且成本高昂。此外，这也可能意味着解决重要的隐私和数据驻留问题。

从成本和复杂性的角度来看，如果一个平台能够连接到您的数据所在的位置，而无需移动数据，绝对是有益的。这种方法可以补充您的现有工具，帮助您实现投资收益的最大化，同时仍然可以提供集中式视图并访问已分散在各种工具中的数据。

**2 您是否可以在内部、公有云或私有云中部署平台?**

许多安全平台仅作为基于云的软件即服务 (SaaS) 解决方案提供。尽管这可能是正确的方法，但许多组织尚未就仅使用云的解决方案做好准备，因此可能需要借助混合多云架构的灵活性。由于许多组织的工作负载仍在内部，因此可灵活地在内部、公有云或私有云中运行的安全平台是一种比较好的选择。与其拘泥于单个部署选项，倒不如寻找一种可以在混合、多云环境中部署的灵活架构。

**3 该平台是否支持与第三方工具的连接和集成?**

如今，组织会使用各种各样的安全工具，它们不太可能全部来自同一个供应商。某些安全平台仅用于集成特定供应商的工具，因此可能会存在局限性。如果您使用来自许多不同供应商的安全工具，就需要寻找一个支持与一系列安全工具和 IT 工具进行开放连接的平台。您需要寻找包含以下内容的平台选项：

- 庞大的合作伙伴生态系统
- 开放式软件开发套件 (SDK)
- 用于添加您自己的自定义连接的支持服务

这种方法可以帮助您确定平台是否可以与您的工具协同工作，而且有助于减少翻新和替换现有工具的需求。

**4 当您的安全计划更改时，平台是否能够进行相应调整?**

在选择平台时，重要的一点是要考虑具有足够的开放性和灵活性，进而能够为您的安全计划提供支持的平台。考虑平台是否能够提供：

- 开放标准
- 开源技术
- 开放连接

开放平台能够连接到第三方工具，而且支持自定义连接和开发。这种方法有助于减少供应商锁定，并促进与多种安全工具和 IT 工具的可互操作性。

**5 它是否能够提供核心编排、自动化和响应功能?**

安全编排、自动化和响应 (SOAR) 解决方案通常被定位为平台本身。不过，将 SOAR 功能内置到您的主要安全平台之后，这些功能会变得更强大，而不是单独提供。因此，您需要寻找一个以 SOAR 作为核心功能的安全平台，以帮助您提高安全团队在一系列工作流程和安全用例中的效率。

**6 它如何支持威胁情报的集成?**

安全分析师经常使用各种威胁源和不同的产品来梳理威胁情报，并为他们的研究和决策提供依据。因此应考虑安全平台是否能提供威胁情报报告，以及这些情报如何与其他功能相集成。将威胁情报集成到您的安全平台之中，不仅有助于减少安全分析师的工作量，还有助于他们做出更迅速、更明智的决策。

**7 供应商是否能够提供软件以外的服务?**

虽然安全平台是一个功能强大的工具，但您可能会发现您还需要组织或安全计划特定的其他服务。安全服务有很多选项，但是如果从还可提供其他安全服务的供应商中选择安全服务，能够让您更轻松地添加这些服务并将其与您的安全平台相集成。

## 了解您的核心安全平台的需求

平台方法可以成为简化安全数据、工具和团队的一种方式。不过，由于可用的选项有很多，因此在考虑哪种安全平台适合您的组织时，重要的是您要找出以下这些关键问题的答案：

- 您是否能够将数据保留在原位？
- 您的部署是否支持混合多云架构？
- 您是否需要开放的集成以及与其他安全工具或 IT 工具的连接？
- 您是否可以随着安全计划的更改轻松地进行调整？
- 您是否能够从安全编排、自动化和响应功能中受益？
- 如何整合威胁情报？
- 除了软件之外，您的供应商是否还能提供安全服务？

## IBM Cloud Pak for Security：专为混合多云世界而构建的互联安全解决方案

IBM® Cloud Pak™ for Security 是一个开放的集成式安全平台，可针对当前及未来跨多个环境的威胁提供深入洞察力。您可以搜索威胁、编排行动并自动执行响应，而无需迁移数据。

借助开放标准和 IBM 的创新成果，IBM Cloud Pak for Security 使您能够访问 IBM 和第三方工具，跨云端或内部位置搜索威胁指示器。IBM 通过 OASIS 开放网络安全联盟贡献 IBM Cloud Pak for Security 中所用的开源代码技术，并与数十家公司建立了合作关系，以提升可互操作性并减少供应商锁定。

IBM Cloud Pak for Security 由与 RedHat® OpenShift® 企业应用平台进行了预集成的容器化软件组成。通过这种集成，它可以在内部及私有云或公有云中运行。借助所包含的 SOAR 功能，IBM Cloud Pak for Security 可帮助您实现安全响应的编排和自动化。

## 了解有关 IBM Cloud Pak for Security 的更多信息

访问 IBM Cloud Pak for Security 网页，了解如何发现隐藏的威胁并做出明智的基于风险的决策，以便对团队的时间进行优先排序。

此外，如果您需要其他人才和技能来支持您的团队，则可以利用 IBM Security 的服务来帮助制定可靠的战略并实现安全计划的转型。





IBM Corporation
New Orchard Road
Armonk, NY 10504

美国印刷
2020 年 1 月