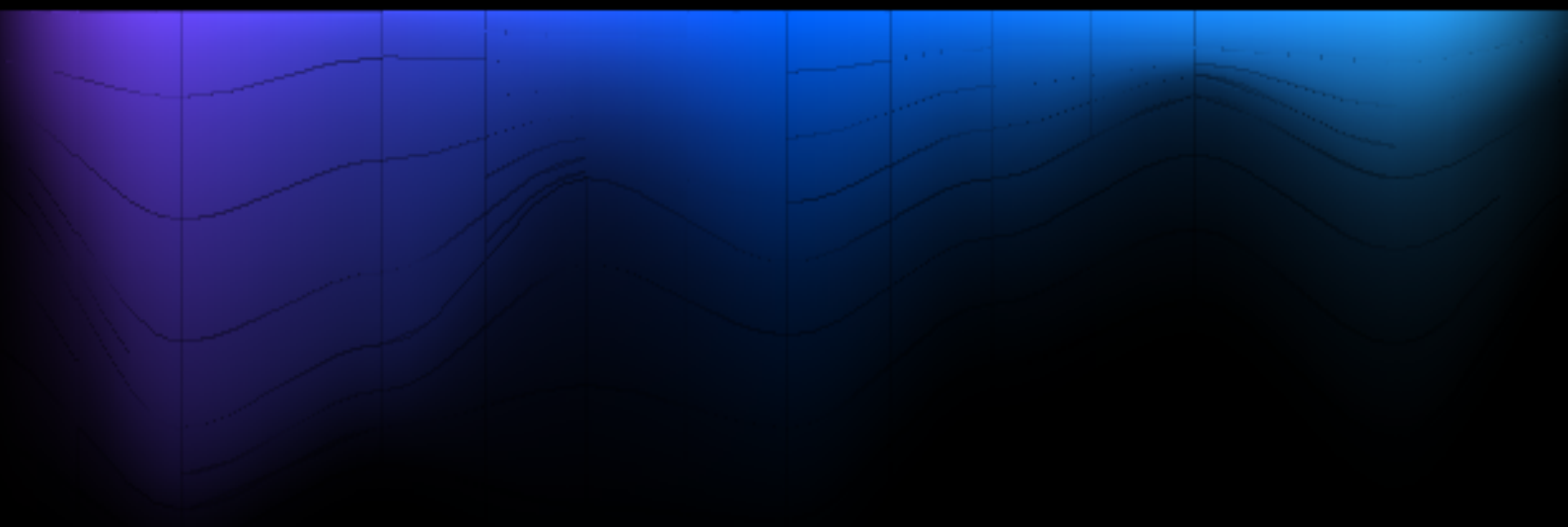
买家指南

全球托管安全服务提供商：比较

您的供应商是否符合这八个条件？您最好选择哪种托管安全服务提供商 (MSSP)？利用这些问题评估您的选项。



IBM Security

IBM

MSSP 供应商要考虑的八个问题

为了在全球经济中参与竞争，企业必须快速创新并高效运营。网络安全工具和服务有助于企业的发展。MSSP 应该提供专业知识和领先的技术，并能够向您的业务负责人、利益相关者和客户证明投资的价值。MSSP 应满足首席监管官和首席合规官的风险和合规需求，并帮助首席信息官 (CIO) 和首席信息安全官 (CISO) 实现安全目标。在解决这些问题并选择供应商时，请查看以下八个问题和答案，它们与适用于企业运营的可用服务有关：

1.

MSSP 供应商提供了哪些有意义的指标与贵企业基于风险的安全战略直接相关?

无分析 - 只是监控安全事件。

(1 分)

不全面的解决方案

该 MSSP 供应商可以告诉您企业存在哪些安全漏洞。除了这些信息外，供应商没有针对这些风险和未来风险的可能性和影响，为您提供任何建议。

进行了分析，但是客户必须确定安全事件的优先级，并确定实施的策略和要采取的措施。

(2 分)

缺乏知识

随着数据的增加，您能够更好地评估数据中的潜在威胁。尽管如此，供应商仍不会为您提供解决安全事件的建议。

客户获得主动管理威胁的预防方法和响应措施，同时牢记底线。

(3 分)

全面的服务

该供应商为您提供包括风险、建议、策略和规则在内的系统管理。MSSP 会检测、响应和报告威胁，并提供相关数据，反映出风险给企业带来的代价。

2.

该解决方案与您现有的技术投资的集成度如何?

该解决方案是一款独立的产品。

(1 分)

有限的功能

如果 MSSP 供应商的系统无法与您的任何其他服务或一流技术产品互联，这会妨碍其产品的有效性。您必须采取额外的步骤来安装新设备，这些设备可能会占用资源，导致您无法开展任何安全工作。

您可以使用您的某些技术来部署其托管安全服务。

(2 分)

零碎的合作

借助这些解决方案，您可以在一定程度上与 MSSP 共享服务或一流的供应商产品。问题在于，供应商的产品与您的工具之间的某些不兼容性可能得由您自己靠其他方式来解决。

产品管理、开发、安全运营中心和您的技术之间有着紧密的合作关系。

(3 分)

可扩展且表现出色

随着贵企业推进数字化转型或云迁移，供应商设计的安全战略也能随之演变。顶尖的 MSSP 供应商能够支持各种产品，并培养了一种合作文化，确保他的工具能满足您的需求。

3.

供应商是否提供先进且全面的安全事件监控技术选项？

客户仅获得基本的安全事件监控功能。

（1 分）

一款解决方案仅适用于某些场景

如果供应商没有用于安全保护的分层或附加组件，他们似乎不太可能响应贵企业的变更。您将获得 MSSP 针对其他任何业务（无论其规模或范围如何）所采用的最低限度客户服务。该 MSSP 具有独立于客户端环境的标准关联规则，但缺乏定制解决方案。

客户有几个选项，但没有一个选项提供了全面的解决方案，包括发现、监控、建议以及安全事件和威胁的预防。

（2 分）

缺少一些项目

由于提供商无法灵活地提供全面的安全监控和保护，因此企业领导可以轻易发现缺点。如果不进行个性化设置，即使是 MSSP 的顶级产品也无法解决您可能遇到的一些紧迫且反复出现的安全问题。

客户获得了广泛的选择，例如发现、监控、分析和保护，包括分布式拒绝服务（DDoS）防范、高级威胁情报（暗网监控）以及身份和访问管理。

（3 分）

广泛的选择

最全面的 MSSP 提供综合的安全管理和监控以及其他功能，例如威胁情报、事件响应和威胁搜索。他们可以全天候（24/7）快速应对您的紧急情况，并提供全方位的可定制服务，用于满足您的风险、合规性和安全性需求。

4.

供应商是否提供定制的本地地域服务交付？

没有这样的定制产品和服务。

（1 分）

全部都有或者可能全部都没有

一些提供商在其全球服务区域中提供相同的托管安全服务。无论贵企业需要什么，这些供应商都提供有限的定制服务和标准服务。

在某些区域交付本地服务。

（2 分）

提供部分帮助

这些供应商的员工会说某个地区或国家的主流语言。这种设置可以带来更高的客户参与度和满意度，但仅限于所服务的国家/地区。

供应商采用本地化方法，拥有全球化规模。

（3 分）

广阔的视野

您希望供应商能够理解您各个层面的业务需求。最强大的 MSSP 在为您定制安全解决方案时，会考虑您周围的本地文化和世界文化。这些 MSSP 还了解全球的法规、数据和隐私要求。

5.

供应商是否提供现代化数字体验并帮助您掌握安全运营中心？

提供商没有推出移动应用。

（1 分）

访问延迟

假如 CISO 或 CIO 在办公室外收到安全事件警报，他们只能使用笨拙的响应流程。连接笔记本电脑、登录 MSSP 门户并找到案件或凭单，这个过程很麻烦。

供应商有移动应用，但加载速度慢，交互性和结果可视性不足，或两者兼而有之。

（2 分）

可用性不确定

在解决安全威胁时，时间是关键。如果服务的应用阻碍了您快速采取行动，缺少作出决策所需的所有必要信息或两者兼而有之，那么您会发现其功能无法满足您的需求。

客户获得了全天候（24/7）可用的应用，该应用可以快速打开并显示详细信息。

（3 分）

随时为您服务

有了可靠的移动应用，您无需笔记本电脑就可以迅速响应安全事件。拿起手机，打开应用，然后开始查看事件的严重性、危急性和背景，以便快速制定决策。

6.

供应商如何应对事件？

事件响应不是 MSSP 的责任。

（1 分）

负担在您身上

该供应商基本上只记录您面临的安全风险及其造成的损害。您必须独自决定如何处理事件或与其他供应商合作。唯一可以肯定的是，这需要您额外投入时间和资源。

供应商提供远程或现场响应选项。

（2 分）

一半答案

您需要在这方面具有灵活性。贵企业需要应对一些复杂的安全事件。还有一些事件出现时，贵企业需要立即获得协助。该 MSSP 可能无法为贵企业提供足够的响应。

供应商可以在远程和现场响应。

（3 分）

防御准备就绪

该提供商几乎可以防范企业面临的任何安全攻击，并提供托管的检测和响应服务。提供此附加服务的顶级 MSSP 还使用系统危急性评分，了解漏洞事件的背景，旨在防范类似事件。

7.

MSSP 能否跨混合多云环境提供集中式策略和可视性?

供应商仅针对企业内部环境提供服务。

（1 分）

洞察力不足

专家一致认为，大多数企业要求的安全监控服务范围包括通过云端交付的服务。无法在公有云或私有云中管理贵企业安全事件的供应商不能满足您当前的 IT 安全要求。

MSSP 提供内部服务和基础架构即服务 (IaaS)。

（2 分）

仍有一些漏洞

如果您广泛使用了平台即服务 (PaaS) 和软件即服务 (SaaS)，则您需要确保 PaaS 和 SaaS 的安全性与 IaaS 的安全性相当。举例来说，该 MSSP 无法监控和检测您的基础结构或大多数第三方应用中的威胁。

您可以完全覆盖混合多云环境，包括 IaaS、PaaS 和 SaaS。

（3 分）

适用于云环境

该 MSSP 拥有专业技能和专业知识，能够处理所有云环境的复杂性。该供应商可以监控和响应支持微服务与容器化平台（比如热门的开源容器应用平台 Red Hat OpenShift）的现代化云原生应用面临的威胁。

8.

供应商使用何种程度的基于机器学习的安全分析来检测事件并确定事件的优先级?

未使用机器学习。

（1 分）

落后于人

现在，许多安全检测设备都使用机器学习，更高效地为客户提供服务。如果供应商的服务中没有该功能，那么贵企业只能频繁且缓慢地响应类似的事件。该 MSSP 将转发大量的噪声和低价值信息需要您处理。

机器学习用途有限。

（2 分）

潜力未尽

该 MSSP 仅将该流程融入了一个或几个安全服务中。该方法不能全面处理有关安全事件的数据，这会导致服务改进时好时坏。

机器学习为供应商检测和预防威胁提供了基础。

（3 分）

做好分析威胁的准备

这种方法为企业提供了自动化安全策略、自动化警报处理和威胁优先级排序功能。通过利用设备分析数据，企业可以及时修复漏洞，防患于未然，并增强针对威胁的预防措施。该 MSSP 能够自动处理低价值的警报和噪音，同时安排分析人员处理高价值和高影响力的警报，让分析人员有更多时间专注于高价值的分析工作。

计分

您的 MSSP 供应商能否满足您所需?

得分：8–15 分，能力不足的利基型提供商

通常，MSSP 供应商缺乏客户期望的许多安全功能，并且可能无法满足您的需求。其受限的功能可能会使得您需要采取更复杂的方法才能遵守法律和行业法规。

得分：6–21 分，试图适应企业需求的利基型提供商

尽管该供应商可能会牢记您的最佳意图，但其服务存在一些限制，因此，他的安全产品存在缺口。您很有可能会发现这些缺失的元素，意识到您需要更全面的解决方案。

得分：22–24 分，久经考验的供应商，具备广泛且深入的知识

即使您不确定您需要什么，该供应商仍能够凭借丰富的经验，为贵企业量身定制解决方案。您将获得灵活的安全信息和事件管理 (SIEM) 技术选项。随着贵企业在全球的扩张，这些选项能够随时满足您的需求。顶级供应商能够帮助企业认识到业务计划中的风险和缺陷，然后再全面实施业务计划；他们能成为企业信赖的合作伙伴，在全球范围内提供专业知识和响应能力。

选择托管安全服务提供商时，谨记以下八个条件

企业需要主动出击，防范恶意攻击。成功的安全计划需要先进的最新情报以及对当前威胁状况的深入了解。此外，您还需要采用战略性方法来管理安全技术的成本和复杂性，这些技术将用于执行安全事件和日志管理、漏洞扫描，以及电子邮件安全和其他活动。但是，由于当前安全威胁和新的安全威胁种类繁多，企业在试图管理自己的信息安全性时，通常缺乏内部资源，进而无法全天候地保护在线系统。

通过将安全运营外包给 MSSP，企业不需要大力投资技术和资源，就可以利用这些服务提供商提供的专家技能、工具和流程，并显著提高安全性。但是，如何选择适合的 MSSP 来满足您的特定需求呢？在选择托管安全服务提供商时，请记住以下八个条件：

1. 与战略相关的广泛漏洞分析
2. 多供应商支持和对各种产品的支持
3. 高级安全事件监控选项
4. 本地交付和全球规模
5. 移动应用
6. 事故响应服务
7. 云安全性
8. 机器学习与自动化

采取下一步行动

IBM® Managed Security Services 满足了所有条件的最高要求，并提供了高级安全解决方案，帮助您实现近乎实时的安全管理。这些解决方案提供系统和身份监控与管理功能和应急响应功能，并且能全天候防范互联网中最关键的威胁。借助 IBM 的安全服务产品组合，企业不仅能降低风险、成本和复杂性，还能更好地管理合规性。IBM Managed Security Services 解决方案产品组合包括内部的安全管理和监控功能，以及基于云的安全服务产品。此外，IBM 入选 2019 年 Gartner 全球托管安全服务魔力象限的领导者象限，并且“Forrester MSSP Wave 2018”报告也将 IBM 评为领导者。要了解 IBM Managed Security Services 以及它能为您提供的帮助，请访问 **ibm.com/security/services/managed-security-services**

© Copyright IBM Corporation 2019. All Rights Reserved. IBM、IBM 徽标及 ibm.com 是 International Business Machines Corp. 在世界各地司法辖区的注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 站点 ibm.com/legal/copytrade.shtml 上的“Copyright and trademark information”部分中包含了 IBM 商标的最新列表。