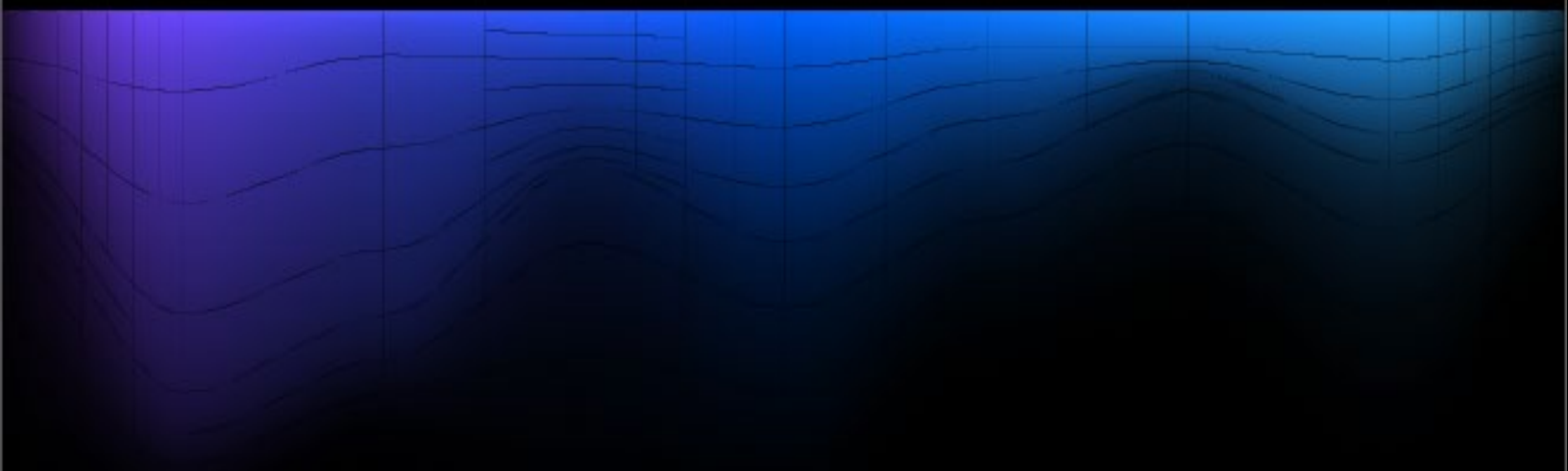
购买者指南

全球托管安全服务提供商：比较

您的提供商是否满足以下八个标准？什么样的托管安全服务提供商（MSSP）是您的最佳选择？通过回答以下问题评估您的选择。



IBM Security

IBM

选择 MSSP 提供商须考虑的八个问题

要想在全球经济中参与角逐，企业必须快速创新和高效运转。网络安全工具和服务有助于推动业务发展。MSSP 应提供相应的专业知识和领先技术，且能够向企业领导、利益相关方和客户证明这笔投资的合理性。MSSP 应满足首席监管官和首席合规官的风险及合规需求，并实现首席信息官（CIO）和首席信息安全官 (CISO) 的安全目标。为解决这些问题而选择提供商时，请查看以下关于贵方业务所适用服务的八个问题及相应的答案。

1.

MSSP 提供商提供了哪些与基于风险的安全战略直接相关的重要指标？

没有分析 — 它仅涉及安全事件监控。
（1 分）

不完整的解决方案
这类 MSSP 提供商可以指出企业存在的安全漏洞。除这些信息外，这类提供商不能就安全漏洞和未来风险的可能性及影响为您提供任何建议。

开展分析，但客户必须分清安全事件的主次，确定要执行的策略和要采取的行动。
（2 分）

知识缺乏力量
随着数据的增长，您会提高对数据中潜在风险的评估水平。但是，这类提供商不会为您提供解决安全事件的建议。

客户获得主动防御方法和响应能力，管理风险的同时能够兼顾盈利。
（3 分）

完整的服务
这类提供商为您提供系统管理，包括风险、建议、策略和规则。这类 MSSP 能够检测、响应并报告威胁，如果风险未得到解决，还会提供反映企业成本的数据。

2.

该解决方案与您现有技术投资的整合情况如何？

该解决方案是独立产品。
（1 分）

有限的功能
MSSP 提供商的系统不能与您的任何其他服务或一流技术产品连接，因而妨碍了这些产品的有效性。您必须额外采取措施安装新设备，这会导致还未开展任何安全工作便已耗尽自身资源。

您可以将它的托管安全服务与自己的一些技术部署在一起。
（2 分）

断断续续的合作
通过这些解决方案，您可以在一定程度上与 MSSP 共享各种服务或一流提供商产品。问题在于这类提供商的产品与您的工具之间可能会出现某些不兼容，导致您需要在其他地方寻求解决方法。

产品管理、开发、安全运营中心和技术之间存在紧密的合作关系。
（3 分）

可扩展和个性化
这类提供商设计的安全战略可以随着您企业的数字化转型或云迁移进程而不断发展演变。顶级 MSSP 提供商秉持与产品无关的原则，培养一种合作关系文化，旨在让他们的工具能够满足您的需求。

3.

安全事件监控技术选项有多先进和全面？

客户只能获得基础的安全事件监控服务。
（1 分）

“一刀切”并不完全适用
不提供安全保护层或附加组件的提供商，似乎不可能适应企业中的变化。您将获得最低配的客户服务，与这类 MSSP 用于其他任何企业（不论规模或范围如何）的服务毫无差别。这类 MSSP 拥有独立于客户环境的标准相关规则，缺乏定制解决方案。

有几个选项，但是没有一个选项能够提供全面的解决方案，涵盖安全事件及威胁的发现、监控、建议及防范等各个方面。
（2 分）

行动有所欠缺
如果提供商缺乏灵活的方法来提供全面的安全监控和保护，那么企业领导很容易就能找到缺陷。如果缺乏个性化能力，即使是这类 MSSP 最高级的产品，也无法解决您可能遇到的一些迫在眉睫且重复出现的安全问题。

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

广泛而全面的选择
最完善的 MSSP 提供全面的安全管理与监控，以及威胁情报、事件响应和威胁捕捉等其他功能。他们能够以 24/7 方式全天候快速解决您的燃眉之急，并提供全套可定制的服务，满足您的风险、合规和安全需求。

4.

这类提供商是否提供量身定制的本地地理服务交付？

没有此类定制化服务。
（1 分）

全有或可能全无
有些提供商在其全球服务区域内交付相同的托管安全服务。这些提供商提供有限的定制水平和不考虑实际业务需求的标准服务。

仅在选定区域提供本地服务交付。
（2 分）

提供局部帮助
这些提供商拥有会讲某个地区或国家内的主流语言的员工。这种安排有助于增进互动，提高客户满意度，但仅限于所服务的这些国家或地区。

这类提供商兼具本地方法和全球规模。
（3 分）

广泛的视角
您希望提供商能够全方位地深刻理解您的业务需求。最强大的 MSSP 会考虑您所处的地域环境和全球文化，为您量身定制安全解决方案。这些 MSSP 还会放眼全球，了解监管、数据和隐私方面的要求。

5.

提供商是否提供现代数字化体验，并让您能够掌上操控安全运营中心？

这类提供商不提供任何移动应用。
（1 分）

访问延迟
负责使办公场所远离安全事件警报的 CISO 或 CIO 面对的是运转不灵的响应流程。连接笔记本电脑，登录 MSSP 门户网站，查找案例或故障单，这种流程带来了诸多不便。

提供一款移动应用，但是加载缓慢，不能提供充分的交互性或结果可视性，或者两者兼有。
（2 分）

不确定的可用性
时间是解决安全威胁的关键。如果一种服务的应用妨碍快速行动能力，缺乏制定决策的所有必要信息，或两种情况兼有，那么您就会发现，它的功能无法满足您的需求。

客户获得一款 24/7 式全天候应用，能够快速打开，便捷显示所有详情。
（3 分）

始终在线，随时服务
借助可靠的移动应用，您无需笔记本电脑就能工作，快速响应安全事件。找到手机，打开应用，开始查看事件的严重性、关键性和相关背景，然后快速制定决策。

6.

提供商如何响应事件？

事件响应不在 MSSP 的工作范围内。
（1 分）

这个重任由您自行承担
这类提供商基本上只记录您面临哪些安全漏洞以及这些漏洞造成的破坏。您必须独自决定如何处理事件，或与其他提供商合作。唯一可以确定的就是，这会耗费您额外的时间和资源。

提供商提供一种选择，要么是远程响应，要么是本地响应。
（2 分）

一半的答案
您需要灵活的响应能力。一些复杂的安全事件需要在企业内进行补救。而另一些事件一旦发生便需要立即获得帮助。这类 MSSP 无法充分响应您的企业的要求。

这类提供商既可以提供远程响应，也可以提供本地响应。
（3 分）

防御措施准备就绪
这类提供商几乎能够防御企业面临的所有安全攻击，提供检测和响应管理服务。提供这种附加服务的顶级 MSSP，还使用系统关键性分数来了解漏洞事件的背景，旨在阻止类似事件再次发生。

7.

MSSP 能否在混合多云环境中提供集中式策略和可视性？

提供商仅为本地环境提供服务。
（1 分）

洞察片面
专家一致认为，大多数企业的安全监控服务需求范围都涵盖在云端交付的服务。无法管理公共云或私有云中安全事件的提供商，就无法满足您当前的 IT 安全需求。

MSSP 提供本地服务和基础架构即服务 (IaaS)。
（2 分）

仍然存在某些漏洞
鉴于平台即服务 (PaaS) 和软件即服务 (SaaS) 的使用较多，它们需要与 IaaS 一样高的安全性。例如，这类 MSSP 无法监控和检测基础架构或源自第三方的大多数应用中的威胁。

您可以覆盖各种混合多云环境，包括 IaaS、PaaS 和 SaaS。
（3 分）

已为采用云做好准备
这类 MSSP 拥有专业技能和专业知识，能够从容应对所有云环境的各类复杂事宜。对于通过微服务和容器化（比如 Red Hat OpenShift，一种流行的开源容器应用平台）提供支持的云原生现代应用，这类提供商可以监控和响应这些应用面临的各种威胁。

8.

提供商在多大程度上运用机器学习进行安全分析，以便检测事件并理清事件的轻重缓急？

未使用机器学习。
（1 分）

落后于潮流
许多安全检测设备现在都使用机器学习来提高向客户交付服务的效率。服务中缺乏这种能力的提供商，会导致您的企业频繁响应类似事件且速度缓慢。这类 MSSP 发送了大量噪音和低价值信息让您处理。

对机器学习的使用有限。（2 分）

未充分发挥潜力
这类 MSSP 仅将机器学习流程整合在一项或几项安全服务中。运用这种方法来处理安全事件相关数据考虑不够周全，这只会导致服务质量参差不齐。

机器学习是提供商提供的威胁检测与防御服务的基础。
（3 分）

为威胁分析做好准备
这种方法可为企业提供自动化的安全策略、自动化的警报处理和威胁优先级划分。通过设备对数据进行分析，可以在漏洞被利用之前及时修复，并增强抵御威胁的防护措施。这类 MSSP 可自动处理低价值警报和噪音，分析人员则可以将更多的时间用在高价值分析上，处理影响重大的高价值警报。

计算总分

您的 MSSP 提供商能否满足您的需求？

分数：8-15 分，能力不足的利基提供商

这类 MSSP 提供商缺乏客户通常期望的许多安全服务，可能无法随着您的需求而扩展。在处理法律和行业法规合规问题时，其有限的功能会让您的工作复杂化。

分数：16-21 分，试图适应各种企业需求的利基提供商

尽管这类提供商可能会考虑您的最佳意图，但它的服务存在局限，导致它的部分安全服务产品存在缺陷。您很有可能会发现这些缺失的要素，并且需要更全面的解决方案。

分数：22-24 分，知识的广度和深度均达标的训练有素的提供商

这类提供商拥有为企业量身定制解决方案的经验，即使您并不确定自己的需求。您将获得灵活的安全信息和事件管理 (SIEM) 技术选项，能够随着您的全球扩张满足您不断变化的需求。顶级提供商可帮助企业在充分实施业务计划之前就认识到计划中存在的风险和缺陷，充当值得信赖的合作伙伴，在全球范围内提供丰富的专业知识和敏捷的响应能力。

在选择托管安全服务提供商时，谨记以下八个标准

企业需要采取主动措施，保护自己免遭恶意攻击。一个行之有效的安全计划，需要即时而周密的情报和关于当前威胁状况的深层洞察。它还需要一种战略方法，用于管理所需安全技术的成本和复杂性，以便进行安全事件和日志管理、漏洞扫描、电子邮件安全和其他活动。但是，面对当前形形色色的新兴安全威胁，试图管理自身信息安全的企业，往往缺乏所需的内部资源，无力全天候充分保护在线系统。

通过将安全业务外包给 MSSP，企业可以充分利用这些服务提供商提供的专业技能、工具和流程，显著增强安全态势，而无需在技术和资源方面进行大量投资。但是，您如何选择满足自身特定需求的合适 MSSP？在选择托管安全服务提供商时，谨记以下八个标准：

1. 与战略相关的广泛漏洞分析
2. 多厂商支持且与产品无关
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. 事件响应服务
7. 云安全
8. 机器学习和自动化

采取后续行动

IBM® Managed Security Services 满足所有条件，在此标准下的分数最高，能够提供高级安全解决方案，实现近乎实时的安全管理。这些解决方案包括系统和身份监控与管理、应急响应以及全天候防御互联网最严重的威胁。IBM 的安全服务产品组合可帮助企业降低风险、成本和复杂性，也可以帮助企业更好地管理合规事宜。IBM Managed Security Services 解决方案组合包括本地安全管理与监控和基于云的安全服务产品。此外，IBM 在 2019 年 Gartner 全球托管安全服务魔力象限中处于领导者象限，而 2018 年 Forrester 的 MSSP Wave 报告也将 IBM 评为领导者。要深入了解 IBM Managed Security Services 以及它能为您做些什么，请访问 **ibm.com/security/services/managed-security-services**

IBM