云安全 2026

挑战、预测及如何获胜

GUIDEPOINT®
SECURITY

目录

执行摘要

[redacted]

您的云安全团队是否正在用昨天的工具和策略应对明天的云战斗？到2026年，人工智能驱动的威胁将以机器速度利用云环境，而你们的人类分析师将努力跟上节奏。在威胁复杂性和防御能力之间的差距不断扩大的情况下，坚守传统安全方法的企业将面临生存的危机。

这不是夸张——这已经在发生了。今年，我们目睹了勒索软件团伙转向攻击云基础设施，并取得了惊人的成功率。与此同时，尽管意识到了问题，但配置错误依然存在。API和供应链为攻击者提供了前所未有的访问权限。而人才短缺使得你正需要专业知识时变得极其脆弱。

组织如果只是对这些趋势做出反应，可能会面临灾难性的安全漏洞，并带来长期的经济和声誉损失。但仍有希望。这份白皮书将探讨未来一年云先行组织将面临的主要挑战。同时，它还提供了成功指南，以及一个帮助您今天开始的清单。

网络安全世界永不停息地变化，你不能坐以待毙。继续阅读，以便在明天威胁到来之前，抢占先机。

你准备好迎接2026年的云安全状况了吗？

- 68%的网络安全威胁分析师报告称，到2025年，人工智能生成的钓鱼攻击将比以往任何一年都更难被检测到。（《SQ杂志》）
- 65%的机构在跟踪和监控第三方集成应用的风险以及纠正SaaS配置错误方面存在困难。（CSA）
- 许多组织（59%）将不安全的身份和危险的权限识别为对其云基础设施的最大安全风险。（CSA）
- 超过三分之一具有人工智能工作负载的组织（34%）已经遭遇过与人工智能相关的违规行为。（CSA）

云安全挑战：2026年版

[redacted]

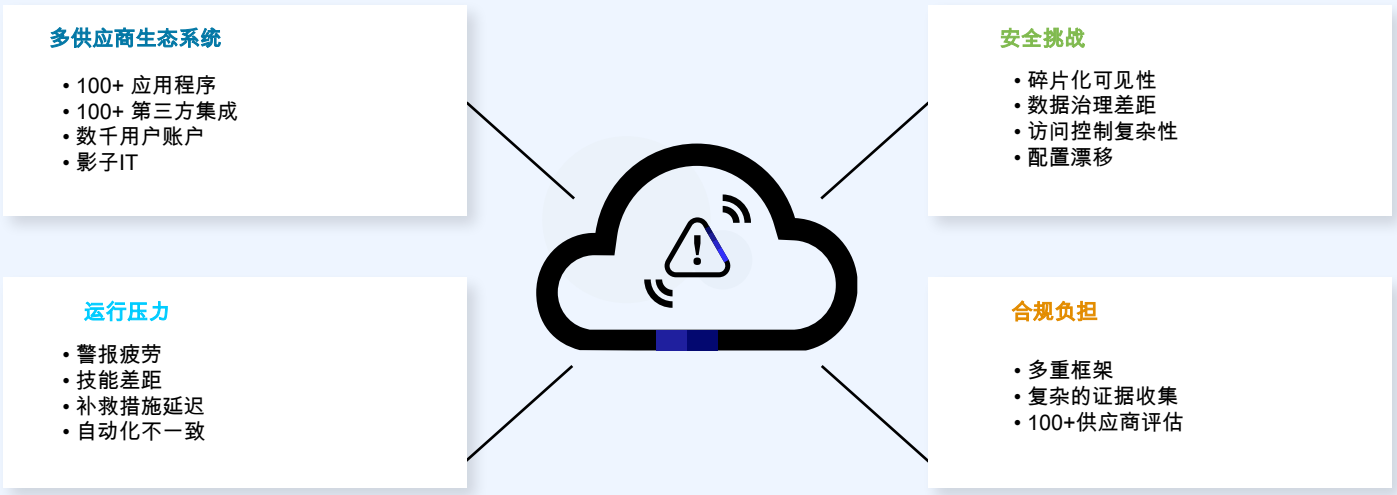
云安全从未简单，而且短期内也不会变得简单。云服务的快速发展不断扩展攻击面，而配置、部署和政策执行中的人为错误仍然是导致安全漏洞的主要原因。展望2026年，组织面临更加复杂的局面：攻击者和防御者都在利用人工智能（AI），攻击手段和技术也在不断演变。

随着技术不断发展，复杂性和持续性的挑战，如SaaS蔓延、供应链风险和配置错误，似乎没有减轻的迹象。再加上持续的网络安全人才短缺，2026年将对即使是弹性最强的安全计划进行考验。以下是我们在未来一年预测你将面临的六大网络安全挑战。

1. 由人工智能驱动的攻击将加剧

作为安全领导者，您正在见证威胁格局的的根本转变。在这场转变中，您所设计的人为防御日益面临机器优化的攻击。这并非理论上的说法；它已经正在改变您对安全计算的看法。

人工智能正在颠覆攻击者的行事方式。机器学习算法现在适应你的防御策略，从失败的尝试中学习，以前所未有的速度和精度利用漏洞。这些系统分析大量成功的渗透数据集，识别出人类防守者可能错过的模式，并将这些洞见应用于对你环境的渗透尝试中。



更令人担忧的是，这些系统是如何从你的防御性回应中学习的。当你阻挡了一种攻击手段，AI驱动的工具会立即转向替代方案，测试各种方法，直到找到成功为止。其影响是显而易见的：你精心策划多年的防御手册，几乎是在实时中被逆向工程和规避。

您多年来精心编制的防守战术手册，正被近乎实时地逆向工程和规避。

经济学也发生了巨大的转变，对防守者不利。人工智能显著降低了发起复杂攻击的成本和技术障碍。曾仅限于国家实体的先进能力正越来越多地被针对您所在环境的犯罪组织所获取。

对于您的董事会和执行领导团队来说，这转化为可衡量的商业风险：之前需要专业知识才能攻破的系统，现在容易受到商品化攻击。您的组织面临着那些以超人类的一致性、以机器速度行动、持续学习和扩大攻击规模超过人类防御者应对能力的威胁行为者。

展望未来，人工智能将处于安全问题的前沿，成为讨论的焦点，最终——解决方案。具有前瞻性的组织将利用人工智能来对抗由人工智能驱动的威胁。没有它，安全团队将陷入一场必败的战斗。

2. 勒索软件将继续针对云基础设施发起攻击

勒索软件威胁正在演变，其方向直接将您的云战略置于靶心。威胁行为者已认识到云环境代表着集中价值。一次成功的攻击就能加密大量数据存储，同时破坏多个业务功能。

这次战略转向并非偶然发生。勒索软件操作者正有系统地开发针对云环境的特定变体，以利用传统基础设施与云环境之间的架构差异。这些攻击针对托管服务提供商、共享存储系统和虚拟机集群，以最大化影响和勒索要求。

这种趋势尤为危险之处在于攻击者如何利用云服务互联的特性。当勒索软件破坏了您的云管理平面，它就获得了禁用安全控制、修改备份系统以及操纵基础设施本身的能力。这代表着本质上的升级。攻击者不仅要针对您的数据，还要针对您赖以恢复的系统。

案例说明：CloudLock勒索软件活动

2025年3月，CloudLock勒索软件攻击波影响了1200多家组织。与以往专注于加密数据的攻击不同，CloudLock针对的是云编排层和管理API。

云锁尤其致命的地方在于它首先能够破坏云身份系统，然后系统地关闭弹性控制。它关闭了备份机制，删除了快照，并加密了生产和灾难恢复环境。

此外，这次攻击跨越了多租户边界，将单个漏洞转变为影响下游客户的供应链攻击。

具有分段身份系统、空气隔离备份和定期测试的恢复程序的组织展示了最快的恢复时间。这一事件是一个鲜明的提醒，表明云安全需要与传统的IT基础设施截然不同的保护与恢复方法。

攻击模式揭示了对手对云计算架构的深入了解。威胁行为者现在专门寻找云管理凭证、API密钥和配置文件，这些都可以提供特权访问权限。一旦获取，这些凭证使攻击者能够在您的整个云环境中横向移动，在部署加密有效载荷前破坏多个系统。

您组织的启示是清晰的：没有相应安全转型的云采用，将创造一个不断扩大的攻击面，勒索软件运营商正在积极瞄准。您传统的针对本地系统的勒索软件防御措施，可能对这些针对云的攻击提供很少的保护。

您的云计算采用速度和安全成熟度之间的差距为勒索软件行为者创造了完美的机会。缩小这一差距需要从根本上重新思考您如何保护云资产免受日益复杂的威胁。

3. 配置错误将持续存在

随着多云和混合部署成为标准作业流程，安全缺口呈指数级增加。每一项新的服务，容器编排平台或是无服务器功能都可能引入潜在的配置错误，而这可能无法被传统安全工具检测到。挑战不仅在于技术，还在于组织管理。云部署的速度往往超越安全团队验证配置的能力。

显著变化的是这些错误被利用的速度。威胁行为者使用自动化扫描工具，不断探测常见错误，将小疏忽变成重大事件。资产部署后短短几秒钟内，配置错误的资产就成了被利用的大门。

根源原因揭示了一个持续的规律。在快速交付的压力下，开发团队往往在不完全理解其安全影响的情况下复制配置模板。默认设置通常优先考虑功能而非安全，需要明确行动来加固资源。当基础服务如身份管理或网络控制出现配置错误时，影响会级联至整个环境。

这项挑战因云环境的动态特性而加剧。临时资源根据需求不断启动和关闭，使实时安全评估变得过时。今天正确配置的环境明天可能因为常规更新或自动扩展事件而变得脆弱。

商业影响远远超出了即时的安全事件。当配置不断超出既定基准时，合规监管几乎变得不可能。审计发现越来越多地指出云服务配置错误是重大控制弱点，这需要昂贵的整改措施，并可能限制商业活动。

是什么让这个挑战尤其险恶的是，尽管意识到了问题，它依然持续存在。许多组织已经经历了因配置错误引起的安全事件，投入了补救措施，但几个月后仍发现自己面临几乎相同的问题。这些教训似乎没有留下深刻印象，因为潜在的复杂性仍在不断增长。

现实是令人不舒服但很清晰：云环境已经变得过于复杂，无法通过人工进行安全验证。依赖于定期审查、人工清单或点时间评估的组织，正在与配置漂移和迅速扩大的云足迹进行一场必败的战斗。

前进的道路需要从周期性安全验证到持续配置执行、从人工审查到自动化安全网、从反应性修复到预防性架构的根本转变。没有这种转型，配置错误将继续成为你最持久且易受攻击的漏洞。

关键风险：前五大云配置错误

过于宽松的身份政策

当身份策略使用通配符或允许广泛的行政权限时，单个被破坏的账户可能导致整个环境的安全漏洞。组织经常低估权限膨胀的连锁反应影响。

2. 公共访问敏感存储

存储资源被无意中配置为公开访问，持续引发重大数据泄露。这种误配置尤其危险之处在于，单次设置更改就能瞬间暴露数百万条机密记录，通常在数据被访问后才触发安全警报。

3. 禁用日志记录和监控

许多组织发现得太晚，关键的审计日志配置错误或完全禁用。没有全面的日志记录，安全团队实际上被蒙蔽了，无法检测到违规行为，重建攻击时间线，或了解系统是如何被破坏的。

4. 未受保护的基础设施管理平面

当云管理界面缺乏适当的访问控制、多因素认证或IP限制时，攻击者可以直接针对控制你整个环境的系统。这种误配置本质上是将基础设施的主密钥保护在仅由密码构成的防线之下。

5. 网络安全组配置错误

网络配置不当持续允许应受限制的流量。这些变化通常在故障排除或测试过程中引入，这些“临时”更改往往变得永久，允许在整个云环境中进行横向移动，并使敏感服务面临不必要的风险。

APIs已成为现代应用的隐形连接组织，威胁行为者已经注意到这一点。这些程序化界面现在成为针对云环境的高级对手最吸引人的攻击向量。

API漏洞尤其危险的原因在于它们可以直接访问业务逻辑和敏感数据。与具有多个防御层的传统Web应用程序不同，API通常提供直接通往关键功能的简化路径。一旦被攻破，它们就能绕过许多外围防御，允许攻击者利用合法功能的方式，这是安全团队从未预料到的。

威胁已经超越了简单的利用。现在，复杂的攻击针对API身份验证机制、滥用速率限制，并操纵API参数以提取数据或获得未经授权的访问。这些攻击尤其难以检测，因为它们使用合法的API调用，与传统安全检测剧本所遗漏的仅存在细微差异的授权使用方式不同。

到2026年，供应链漏洞的上升势头仍在继续。现代应用依赖于 数十或数百
第三方组件，在您直接控制范围之外创造了一个不断扩大的攻击面。更隐蔽的是，威胁行为者知道供应链依赖于信任关系。

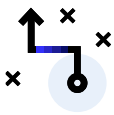
当受到破坏的组件拥有有效签名并来自可信来源时，传统安全控制提供的保护很少。威胁行为者已认识到这些系统相互依赖性作为战略机会，目标是软件开发流程、第三方库和云服务依赖。近年来发生的SolarWinds和Log4j事件并非异常。它们代表了攻击方法的根本转变，这种转变仍在加速。通过破坏供应链中的单个组件，攻击者可以以最小的努力同时影响数千家下游组织。

API与供应链漏洞的叠加导致风险加剧。组织现在面临第三方API被泄露，可能在其应用程序生态系统中引入漏洞的情景。单一脆弱的依赖项可能通过API连接暴露多个系统的数据，而安全团队甚至可能没有意识到这些连接的存在。同时，供应链的漏洞可能持续数月才被发现。

API和供应链漏洞代表着一种 根本威胁 对您云基础设施的完整性和其上运行的应用程序。

应对这些挑战需要将安全关注点进行重大转移。基于传统的以周边安全为框架的模式，对API篡改或依赖系统被破坏的保护几乎为零。组织必须实施能理解API行为的管控机制，监控细微异常情况，并验证供应链中从开发到部署的每个组成部分的完整性。

没有这种转型，您的组织将面临一个不断扩大的盲点，而攻击者正越来越集中精力攻击这个盲点。



设置

2025年1月，成千上万的组织依赖一个流行的API管理平台来处理系统与合作伙伴之间的关键数据传输。

攻击

威胁行为者入侵了平台的身份验证模块，创建后门访问权限的同时确保所有安全测试仍然通过。三个月来，攻击者悄然截获了通过受影响API在380个组织中流动的数据，且完全没有触发警报，因为API调用看似合法。

关键教训

没有对API生态系统和供应链依赖的全面可见性，组织无论在其他安全投资方面如何，都仍然处于脆弱状态。那些拥有API安全监控、依赖验证系统和行为分析的组织，能够更快地发现违规行为并限制其暴露范围。

5. SaaS安全复杂性将达到临界点

到2026年，随着SaaS生态系统复杂性的增加，安全团队将面临前所未有的挑战，传统安全模式将不堪重负。即使在共享责任模式下，供应商承担了一部分安全负担，但随着SaaS应用数量扩展到数十个甚至数百个，组织仍难以维持对安全状况的可见性和控制力。

是什么使得这一挑战特别尖锐的是现代SaaS格局的规模和碎片化。安全负担变得 超出可控制的比重。

机构需要在多云计算环境中协调数十项供应商安全评估、复杂的合规性要求，以及原本就未设计协同工作的不同安全控制的整合。这些碎片化的安全努力在覆盖面上产生了漏洞，使得复杂威胁能够悄无声息地溜走。

挑战超越了简单的工具管理。团队正被来自多个SaaS安全平台的警报淹没，每个平台都提供对云生态系统不同部分的碎片化视图。仅仅向问题投掷工具只会加剧困扰SaaS安全的难题。组织需要战略规划和专家战术执行，以有意义的手段包围SaaS安全，提高可见性，降低运营复杂性，并对警报信号进行规范化，以实现统一的、全面的警报视图。

增加了这项复杂性的是SaaS应用程序本身的不断变化。频繁的更新、功能增加以及API更改意味着安全性配置需要持续监控和调整。昨天看似安全的事物，明天可能暴露出脆弱性，给本就压力山大的安全团队带来永无止境的维护负担。

在SaaS生态系统中的身份治理又是一项重大挑战。员工们经常使用几十个应用程序来完成工作，每个应用程序都有自己的权限模型。使用传统方法来维持最小权限访问几乎变得不可能。应用程序级别的身份和服务账户的激增，将这些工具连接起来，进一步加剧了这个问题，形成了一个传统安全工具难以有效监控的无形访问路径网络。

数据主权和跨应用数据流转也引入了额外的复杂层级。源自某个SaaS应用的信息往往跨越多个平台，造成人们不确定敏感数据驻留何处，以及在其生命周期中如何得到保护。

组织在数据跨越应用边界后往往失去可见性，从而在其安全态势中造成盲点。

技能差距加剧了这些挑战，因为安全专家现在必须了解数十个独特的SaaS平台，每个平台都有其自身的安全架构、API和最佳实践。这种专业知识的维护在日益扩大的SaaS产品组合中变得越来越困难。

6. 对网络安全人才的迫切需求

网络安全技能差距正以令人担忧的速度扩大，导致人才危机，甚至威胁到资金最充足的网络安全项目。

随着云计算的加速采用，对既了解安全原则又熟悉云原生架构的专业人员的需求，创造了一个前所未有的竞争性招聘环境，即使是慷慨的薪酬方案也无法吸引合格的候选人。

这种人才短缺导致安全漏洞不断累积。人手不足的团队在资源不足的情况下，试图监控日益复杂的环境，感到警觉疲劳。关键的安全功能变成了被动反应而非主动预防，形成了容易被熟练攻击者利用的盲点。当有经验的员工离职时，他们带走了关于你环境独特安全态势不可替代的机构知识。即使有经验的新员工加入，这种知识也需要数月时间才能重建。

专业建议：将你的才华集中在战略目标上，其余的进行外包。

最成功的安全组织已经停止了试图通过招聘来解决人才危机的做法。相反，他们采取了一种战略性的方法：将内部人才储备用于需要组织背景的高价值活动，并将标准化的安全功能外包给专业合作伙伴。

与此同时，威胁行为者意识到，人员短缺的安全团队代表着机会，特别是针对在人员变动期间或监控能力紧张时的组织进行针对性攻击。

人才短缺不是暂时的中断，而是一种需要结构性适应的新常态。可持续的前进道路需要一种混合方法，以最大化内部专家的影响，同时利用外部资源进行标准化的安全运营。那些将安全运营模式转变为在约束条件下有效运作的组织将建立起韧性，而那些等待人才市场正常化的组织则越来越容易受到攻击。

预测成功：2026年制胜策略

尽管2026年将带来其份额的挑战，但它也为组织将云安全转化为竞争优势提供了机会。新兴技术正在重塑威胁格局，同时为防御者提供新的工具和情报。安全计划正在从理论走向实践，解决长期存在的问题，如可见性差距、SaaS蔓延和勒索软件的恢复力。

更加整合、有效的策略。同时，向更智能的架构、简化操作和更强伙伴关系的转变正帮助组织克服人才短缺和资源限制。随着这些策略的实施，2026年有望成为安全领导者重新定义韧性并为长期成功奠定基础的一年。

1. 人工智能增强、人工验证的安全将对抗人工智能威胁

我们的预测

组织成功实施人工智能增强、人工验证的安全措施将能够更快地发现威胁、更有效地应对，并维护对日益复杂的攻击的韧性。那些坚持纯手动安全操作或期待人工智能完全取代人类判断的组织将发现自己越来越容易受到攻击。

组织正在利用人工智能对抗攻击者，为日益增长的以人工智能为动力的威胁创造技术平衡。

防御性人工智能系统现在能够快速检测模式和异常，识别出隐藏在大量数据集中、传统安全工具完全忽略的微妙攻击迹象。随着我们继续前进，我们将看到人工智能安全平台的广泛应用，这些平台在云环境中持续搜寻威胁，推荐针对性的漏洞修复，并几乎实时地调整防御以应对不断演变的攻击技术。

然而，最有效的实施并非替代人类专业知识——它们是增强它。新兴的最佳实践是将AI驱动检测与人类验证和决策相结合。

人工智能系统在处理大量安全数据和发现潜在威胁方面表现出色，而人类分析师则提供关键背景，调查复杂场景，并在适当的应对措施上做出细微的决策。

具有前瞻性的组织也在解决防御性人工智能的伦理维度。它们正在实施治理框架，确保人工智能决策的透明度，明确机器辅助安全行动的责任，并定期审计人工智能系统，以发现潜在的偏见或效果偏差。

2. 网络韧性将加强勒索软件预防策略

随着勒索软件越来越多地针对云基础设施，安全领导者正从“不惜一切代价防止违规”转向“即使在出现违规时也要保持运营。”

这种以韧性为核心的策略承认现实：复杂的攻击者最终会突破您的防线，尤其是在复杂的云环境中，一次配置错误就能提供广泛访问权限。

我们的预测

组织在防御和韧性之间保持平衡时，在面对不可避免的云勒索软件攻击时将展现出显著更好的结果。问题不在于你是否会遇到此类攻击，而在于攻击发生时，你将在数小时、数天或数周内恢复过来。

组织建立有效的云弹性时，关注三个关键能力：

- **微细分段，限制横向移动**
- **不可变备份，与生产系统具有独立认证**
- **云特定业务连续性程序，包括离线通讯渠道**

最重要的是，有弹性的组织会定期对其恢复能力进行测试，以应对真实的勒索软件场景。这些演练揭示了关键缺陷，包括与受损害环境共享身份验证的备份系统或需要访问加密系统的恢复程序。

财务合理性非常令人信服。在平衡预防和韧性投资的组织中，成功攻击的整体影响显著降低。当云端勒索软件攻击发生时，三天和三周恢复期之间的差异往往不在于预防技术，而在于韧性准备工作。

3. 综合安全平台将关闭可见性差距

持续存在的云配置问题挑战，要求在安全方法上进行根本转变。

组织正在放弃使用零散的不相连的点解决方案，转而采用专为解决复杂云环境中配置可见性和政策执行而设计的综合安全平台。

这些集成平台为所有云资源提供持续的、全面的可见性。它们在配置错误出现的瞬间就能检测到，而不是在周期性扫描中。通过维护云资产及其安全状态的完整清单，这些系统消除了配置错误通常隐藏的盲区。

我们的预测

采用统一平台的组织将显著降低其配置错误风险。他们不是与配置错误进行无休止的斗争，而是建立持续可见性和自动执行的基础，使安全配置成为默认状态，而不是持续的斗争。

是什么使这些平台特别有效

针对配置错误，它们的强制执行能力是它们的特长。

自动设置安全护栏。当开发人员时，...

使用具有公共访问权限的存储桶或

过度宽松的安全组，平台可以自动修复问题或完全阻止部署，防止配置错误在庞大的云环境中持续存在。此次整合也解决了安全偏差的挑战。

与其说定期合规检查错过了中途的变化，这些平台持续验证配置与安全策略的一致性，确保环境在演变过程中始终保持正确的配置。当策略更新以应对新的威胁时，平台会自动识别所有云环境中受影响的资源。

4. 零信任架构将从理想走向关键

API和供应链面临的日益严峻的威胁需要一种安全模型，这种模型从不假设信任，即使是看似合法的连接。零信任架构已从概念发展成为一个实际、经过验证的现实，为连接的组织提供了确保这些易受攻击组件所需的框架。

我们的预测

零信任将逐渐成为API和供应链保护的主导安全模型，其实施将平衡安全性与运营需求。组织将实施微分段化来隔离关键API、针对供应链整合的即时访问以及连续监控，立即识别内外部连接中的可疑活动。

对于API的安全性而言，成熟的零信任实施会验证每一个API请求，无论来源如何，对每一次交互都实施持续的身份验证和授权。这种方法消除了传统的安全边界，这使得经过身份验证的用户可以不受限制地访问API。相反，每一次API调用都会基于身份、设备状况、请求模式和数据敏感度进行单独的验证。这种警觉性甚至在使用有效凭证的情况下也能检测到异常行为。

为了供应链安全，零信任原则强制在允许集成之前对每个组件进行严格的验证。这包括对软件签名的自动化验证、对第三方行为的持续监控以及限制潜在损害的动态访问限制。最重要的是，成熟的实施假定即使是可信的供应商也可能受到损害，实施控制措施以限制供应链攻击的破坏范围。

关键进步将是将这些原则无缝融入开发工作流程中，使零信任验证成为API部署和第三方集成的自动部分，而不是安全瓶颈。

5. SaaS安全转型将降低复杂性

正如我们十年前见证云计算安全领域的变革一样，SaaS安全正在经历一场根本性的转型。

在早期云时代，组织部署了分散的工具来管理配置、保护工作负载和进行身份治理，这导致了可视性的空白并压倒了安全团队。市场最终围绕着将这些分散的控制集成为一致的安全解决方案的统一平台进行整合。

2026年的SaaS安全格局将不会有任何不同。组织在SaaS安全态势管理、身份治理、数据保护和第三方风险方面都面临着孤立的点解决方案的挑战。每一种解决方案都只提供了拼图的一部分。这种方法创造了危险的地带盲点，让威胁行为者可以在未被察觉的情况下进行操作。

我们的预测

SaaS安全复杂性将达到临界点，迫使组织放弃基于工具的孤岛式方法。能够提供整个SaaS生态系统统一可见性和控制的集成、智能驱动的安全平台将占据主导地位，通过与服务提供商合作，组织将进一步提高效率，这些服务提供商专注于大规模的SaaS环境。

随着我们步入新的一年，我们将看到需求增长，针对SaaS安全平台的這些將這些零散的工具整合的全面解决方案。随着需求的集中化的大规模可见性和控制，这些平台将利用人工智能在SaaS生态系统中关联威胁信号，自动化合规映射，并根据业务环境优先考虑漏洞。这一进步不仅将整合工具或日志，还将从根本上改变组织处理SaaS安全的方式。他们将从反应式的点解决方案转变为在整个SaaS领域的主动、集成保护。

第六条：建立战略合作伙伴关系的组织将增强其抗风险能力。

网络安全人才缺口不断扩大，尤其是云安全专家，这要求我们采取超越传统招聘的创新方法。组织机构越来越多地建立战略安全合作伙伴关系，以获取专业知识和扩大能力，克服内部人员编制的限制。

我们的预测

成熟的安全伙伴策略的机构，尽管人才短缺问题持续存在，但将展现出显著的韧性。它们不是与持续的空缺职位抗争或压榨有限的工作人员，而是利用一个专门合作伙伴的生态系统，这些合作伙伴共同提供与它们特定需求和风险概况相匹配的全面安全能力。

这些合作远远超越了传统的供应商关系。具有前瞻性的组织正在与托管安全服务提供商、云安全专家和咨询公司建立深度合作，这些公司真正成为其安全团队的延伸。这些安排提供了获得专业云安全技术的途径，无需面临直接招聘的挑战和薪酬溢价。

现代安全合作伙伴之所以特别有效，是因为它们融入了日常运营。这些关系并非孤立的互动，而是提供了对云安全架构、威胁狩猎和事件响应等专业技能的持续访问。这种方法使得内部团队能够专注于战略性和特定于业务的网络安全需求，而合作伙伴则处理专业或资源密集型功能。

这些合作伙伴关系也在解决困扰行业的知识转移挑战。领先的组织将他们的安全合作伙伴关系结构化，包括导师制、培训、

并且是那些随着时间的推移构建内部能力的协作项目。这种方法在提供即时安全覆盖的同时，逐渐培养关键领域的内部专业知识。

2026年云安全准备清单

投资人工智能安全能力

- [ ] 建立人工智能安全的数据基础，通过集中日志和警报 Develop expertise in AI security through targeted hiring and training programs
- [ ] 从小规模的专注AI应用案例开始，例如钓鱼检测或用户行为分析。
- [ ]
- [ ] 实施解决人工智能治理政策的措施。道德使用和潜在偏见

成功看起来像： 利用人工智能助手以5倍于人工方法的速度调查警报，并在攻击影响运营之前预先阻止80%的攻击。

加强云基础设施保护

- [ ] 部署攻击者无法加密或删除的不可变备份系统
创建包含离线通信计划的勒索软件专用剧本
- [ ] 执行自动化恢复测试以验证恢复能力，为新的云资源建立默认安全模板。
- [ ]
- [ ]

成功看起来像： 将勒索软件恢复时间从数周缩短至数小时，并在攻击期间保持业务连续性。

地址配置管理

- [ ] 实施基础设施即代码，并进行预部署安全验证
建立持续合规性检查，并实施自动化修复
- [ ] 部署跨所有环境的云安全态势管理工具
为新的部署创建云安全架构审查委员会
- [ ]
- [ ]

成功看起来像： 在六个月内将误配置减少90%，并在它们被利用之前自动修复剩余的10%。

提升第三方风险管理

- [ ] 清点所有API和第三方依赖项
with comprehensive software bills of 材料（软件物料清单）
- [ ] 实施API网关保护以及第三方代码自动化扫描
- [ ] 部署运行时API安全监控以检测异常行为
- [ ] 建立供应商安全评估程序并进行持续监控
- [ ] 需要在部署前对所有新的API和第三方集成进行安全测试。
- [ ] 制定专门针对API和供应链妥协的应对计划
- [ ] 实施API版本控制和弃用流程，以消除遗留漏洞

成功看起来像： 全面洞察API流量模式和易受攻击的组件，在攻击尝试触及应用程序后端之前自动阻止，以及能够在漏洞披露后数小时内隔离受损害的依赖项。

确保您的SaaS生态系统安全

- [ ] 清点并分类贵组织所使用的一切SaaS应用程序
- [ ] 通过SaaS安全态势管理（SSPM）解决方案实现集中式可见性和控制。
- [ ] 始终一致地在SaaS应用中实施最小权限和基于角色的访问控制。
- [ ] 自动化监控配置错误、数据共享以及影子IT检测

成功看起来像： SaaS应用统一可见性，主动识别误配置，并在数据泄露前解决风险的能力。

处理当前云访问

- [ ] 审核现有身份系统中的未使用账户和过度特权
- [ ] 实施即时访问管理功能的配置
- [ ] 全面部署多因素认证系统。
  云资源
- [ ] 建立持续的接入监控和异常检测

成功看起来像： 消除95%用户的站内特权，并自动检测和拦截凭证泄露尝试。

建立战略合作伙伴关系

- [ ] 加入特定行业的安全威胁情报共享组
  与关键云服务提供商建立直接的安全通道
- [ ] 建立与安全服务机构的关系
  与同侪组织建立互助协议
- [ ]
- [ ]

成功看起来像： 获得针对您环境的可操作指导，并在重大安全事件期间确保能够访问事件响应资源。

结论

随着2026年云安全挑战的加剧，组织站在一个关键的十字路口。由AI驱动的攻击、日益复杂的勒索软件、持续的配置错误、API暴露以及不断增长的SaaS复杂性，带来了前所未有的风险。加上持续的网络安全人才短缺，许多团队在单独应对这些威胁时压力过大。

GuidePoint Security uniquely positions itself to help you meet this moment. Our cloud security services integrate deep technical expertise with strategic guidance, enabling organizations to:

- **利用经专家人类验证增强的人工智能防御。**
- **构建减少勒索软件和其他高级威胁影响的韧性策略。**
- **将分散的工具整合到统一平台上，恢复可见性和控制。**
- **定制的成熟零信任框架，适用于您的云生态系统。**
- **通过集成、端到端保护简化SaaS安全。**
- **通过灵活的合作模式，以专业云人才增强内部团队。**

与GuidePoint Security合作，您获得的不仅仅是解决方案，更是一个值得信赖的合作伙伴，我们致力于您的成功。我们经过验证的方法论、专业的实践者以及以结果为导向的服务，将赋予您信心，帮助您应对当今的复杂局面，并为未来的挑战做好准备。

云计算安全未来将回报那些将创新与专业知识相结合的人。有了GuidePoint Security的支持，您可以将风险转变为韧性，确保您在日益复杂的数字世界中占据一席之地。

GUIDEPOINT®
SECURITY

1900 Reston Metro Plaza，705室，雷斯顿，VA 20190 guidepointsecurity.com • i
nfo@guidepointsecurity.com •（877）889-0132 WP.CS26.2510