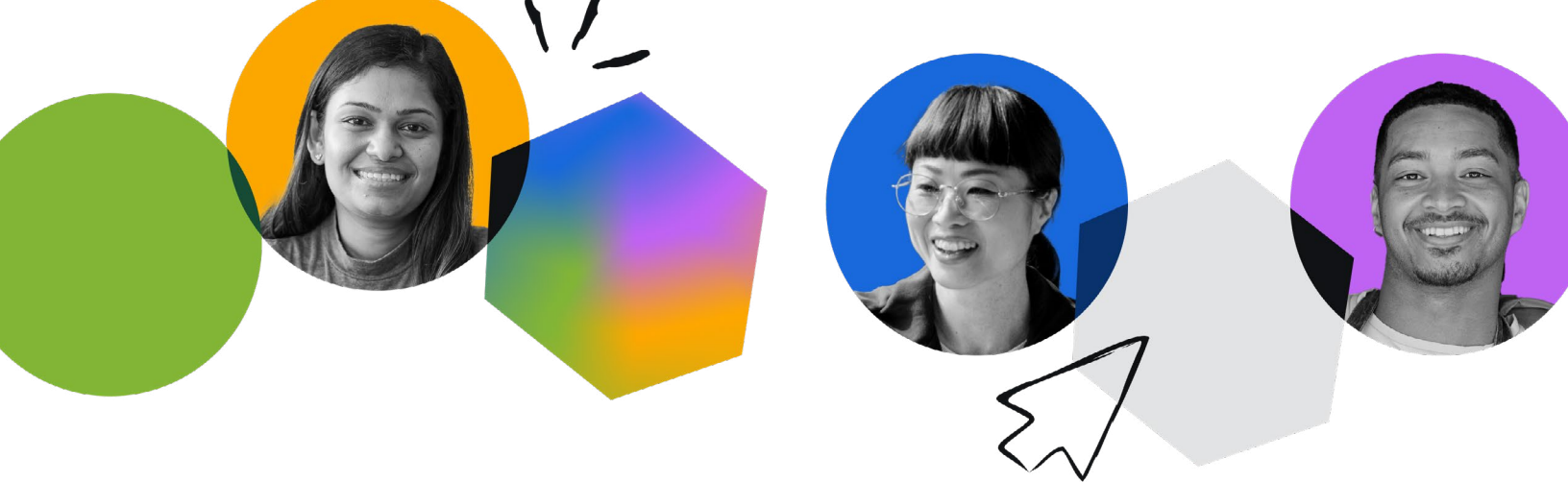
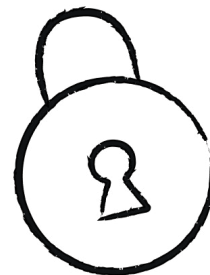




# 释放 Atlassian AI 潜能， 确保数据安全无忧

人工智能（AI）正在以史无前例的速度改变团队协作模式。借助 AI 的力量，团队现在能够更快速地获取信息、加速跨部门决策，并打造更优质的客户解决方案。在未来三年内，**92% 的企业计划增加对 AI 的投入**。AI 采用率的飞速增长，意味着企业需要采取主动措施，解决 AI 带来的安全性与合规性挑战。为了高效实现这一目标，企业应建立一种基于多层策略的、值得信赖的 AI 使用方法。

当您准备在全公司范围内推广 AI 时，请参考您目前评估其他可信云服务商时所遵循的核心原则。许多行业标准的安全、隐私和合规准则，都为评估和实施 AI 解决方案提供了坚实的多步基础。在本指南中，Atlassian 将深入探讨几个关键考量因素，帮助您了解我们的信任体系及其在 Atlassian Rovo 中的应用，并介绍您可以使用的各项控制功能，助您信心十足地开启 Atlassian 云端的 AI 功能。



# 优先构建全组织范围的可见性

看不见，便无法保护。请赋予您的管理员和安全团队所需的可见性，以便他们高效管理 AI 权限与活动。

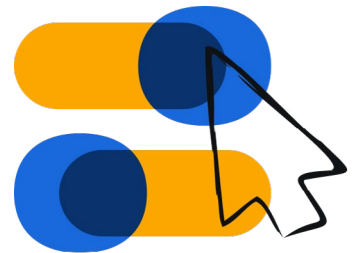
深入了解用户可访问的信息，对于有效规避风险和保护数据安全至关重要。当企业能够跨部门建立强大的数据连接时，AI 才能发挥最大效用。为 AI 解决方案提供更丰富的上下文信息，能显著增强团队间的协作，从而更快速地获取跨项目洞察，最终达成更高效的业务成果。

为了让您的组织做好迎接 AI 的准备，准确识别并分类数据至关重要。在启用 AI 之前，企业迈出的第一步应当是：明确数据的存储位置、访问权限归属以及敏感数据的占比。

这些最佳实践同样适用于您正在评估的所有软件供应商。具体到提升 Atlassian 产品组合的可见性，我们提供了多个仪表板（Dashboard），帮助您审查并维持对 Atlassian 云端环境的全局掌控。

## 最佳实践落地指南：

- ✓ **Atlassian 管理后台的组织洞察仪表板（Organization Insights Dashboard）**：允许您查看与组织关联的 Jira、Jira Service Management 和 Confluence 云端产品的日活及月活用户数。
- ✓ **Confluence 中的 Mission Control 功能**：助您轻松掌握谁拥有管理权限或外部访问权限，并监控空间数量、功能使用情况以及站点内的高频消费内容。
- ✓ **组织洞察仪表板中的 AI 洞察页签**：针对 AI 驱动的 Rovo 功能提供深度可见性，追踪其随时间的使用趋势。您还可以利用这些数据识别使用缺口，帮助更多团队接入 AI 能力。



# 原生安全：兼顾隐私与合规

AI 解决方案的开发应当遵循与其他云产品相同的严谨标准，以确保其满足组织的安全性、隐私性和合规性要求。

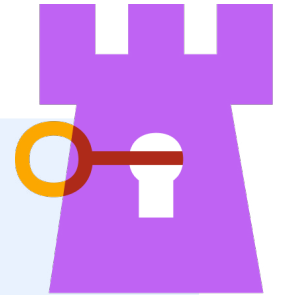
AI 解决方案的开发应当遵循与其他云产品相同的严谨标准，以确保其满足组织的安全性、隐私性和合规性要求。在评估 AI 解决方案时，请明确您组织在引入新云产品时的准则。大多数企业已针对 AI 解决方案建立了一套核心信任要求，涵盖了安全、隐私和合规等方面。随着 AI 的快速演进，许多云服务提供商已将其 AI 解决方案的开发与负责任的技术或人工智能伦理原则挂钩。审查这些原则有助于您更深入地了解各家机构在 AI 解决方案的安全与隐私设计上采取了何种方法。

此外，建议深入调查您的数据将如何被使用、存储和共享。您的解决方案提供商应当在这些方面保持透明，并就数据处理方式提供明确保证。

Atlassian 的 AI 策略根植于其**负责任技术原则**

以下是 **Atlassian** 保护您数据的方式：

- ✓ **多元化模型架构：** 结合使用 Atlassian 自托管模型（如 Mixtral、Phi 和 Llama-3）及第三方大语言模型（LLM），包括 OpenAI、Anthropic 和 Gemini。Atlassian 所使用的 LLM 供应商不会保留您的输入与输出数据，也不会利用这些数据来改进其服务。
- ✓ **统一的安全标准：** Rovo 遵循管理所有 Atlassian 产品及平台的相同安全标准与实践。同时，我们提供静态和传输过程中的端到端加密，确保您的数据始终受到保护。
- ✓ **尊重现有权限：** Rovo 严格遵循您所连接的所有第三方产品的既有权限设置。
- ✓ **数据用途限制：** 您的输入和输出内容仅用于为您提供服务并优化您的体验。这些数据绝不会被用于跨客户的 LLM 模型训练。
- ✓ **行业合规认证：** Rovo 持续满足各项监管要求，包括 SOC 2 和 ISO 27001 认证。



# 强化数据管控

建立全公司统一的标准，助力您精准掌控数据存储位置、访问权限及使用方式。



在完成组织评估并掌握用户与数据现状后，接下来的关键步骤是评估权限与管控机制。为了最大限度降低用户误触非授权内容的风险，Atlassian 强烈建议您对现有的用户权限和内容策略进行审计。一旦组织识别出特定类型的敏感数据，就应当实施并执行相应的管控措施。通过设置数据访问控制，可以降低组织的整体风险，确保只有获得授权且有业务需求的人员才能访问相关数据。

在使用 Rovo 时，您可以设定相关策略，在为 AI 提供必要的上下文和数据支持以强化协作的同时，确保现有的权限体系和数据敏感度等级得到严格遵守。

## 助您信心十足地管理 Rovo 的管控功能与设置：

- ✅ **权限对齐：**Rovo 严格遵循您在 Atlassian 产品及第三方连接器中设置的权限。用户仅能看到其原本就有权访问的数据。
- ✅ **分级管理：**Atlassian 云端提供“委派管理”体验，允许您在组织、站点和产品等多个层级灵活设置权限。
- ✅ **灵活开关：**您可以随时启用或禁用 AI 功能。只需进入 Atlassian 管理后台，即可在产品层级轻松管理相关设置。
- ✅ **持续审计：**定期审查组织内部的内容，确保全公司范围内的敏感信息访问权限始终处于受控状态。
- ✅ **数据驻留：**支持将 Rovo 的相关产品数据存储在您选择的特定区域，以满足当地法律法规及监管要求。



## 以信任为基石，全面释放 AI 潜能

采取可信的方法推广 AI，并不意味着必须牺牲组织的创新速度。借助 Rovo，您可以在确保安全的前提下，将强大的 AI 能力引入 Atlassian 云产品中。

- ✓ **奠定基础：**迈出关键的第一步，深入了解您组织的当前环境与信任要求。
- ✓ **精细化管控：**设定相关策略与管控措施，以获取团队使用 AI 情况的深度可见性。您可以利用这些洞察赋能团队，鼓励其通过 AI 实现更深层次的协作，并显著提升工作效率。
- ✓ **持续优化：**定期评估组织使用 Rovo 的情况，确保已实施的权限与策略能够持续满足您的安全性与合规性要求。

# 借力 Atlassian 值得信赖的 AI 解决方案，重塑团队协作。

立即联系您当地的 Atlassian 解决方案合作伙伴，信心十足地开启 Rovo 之旅。

