

## Forcepoint CASB

Forcepoint 云访问安全代理 (CASB) 可自动发现云应用程序的使用情况, 分析风险并对SaaS和生产应用程序实施适当的控制。使用Forcepoint CASB, 用户可以获得他们想要的应用程序, IT人员可以获得所需的控制权。

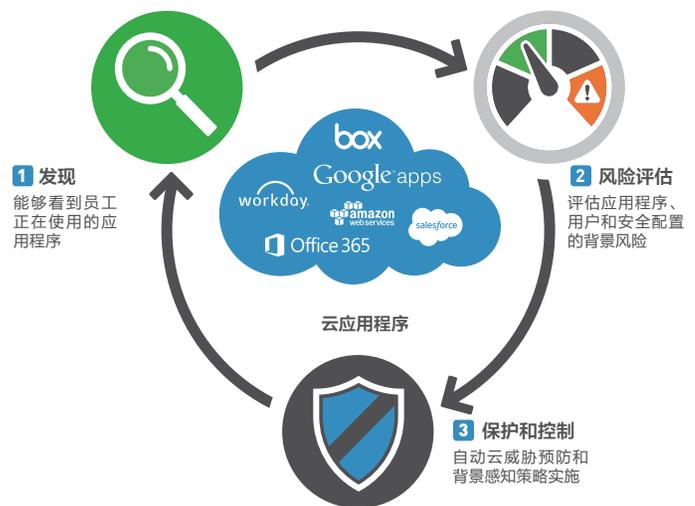
### 通过使用云应用程序提供可视性和控制

云应用程序允许机构降低成本并弹性分配资源, 但也会对安全和合规状况带来风险。随着BYOD的普及, 云应用在工作场所的加速推广, 已经创造了对保证基于云的、经批准的应用程序安全的需求, 如Office 365, Dropbox和Salesforce等。

对于IT来说, 防止数据丢失和强化访问控制是首当其冲的事情。

员工可能是安全风险的主要来源, 因为恶意的内部人员希望利用他们对组织的云应用的无限访问来泄露数据。

Forcepoint确保所有用户和终端对云应用程序的安全和高效使用。

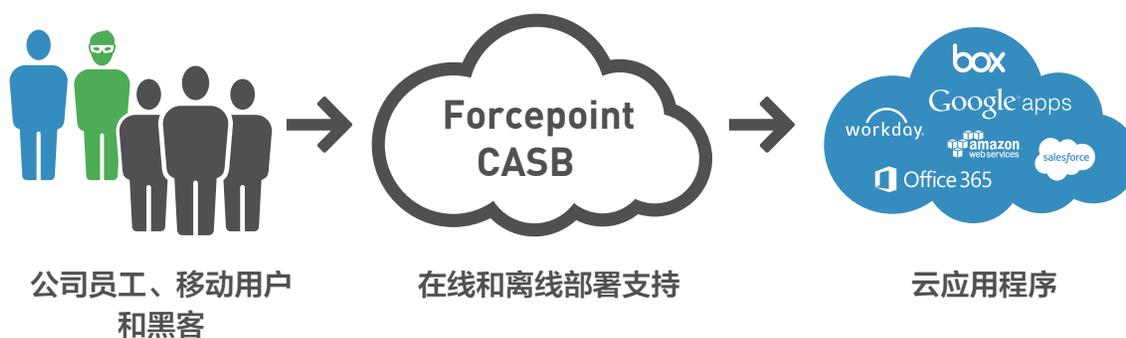


要实现可见性和控制, 需要一个云访问安全代理, 支持应用程序发现、风险管控, 为批准和未经批准的应用程序进行访问控制和数据保护。



## 减轻云应用程序风险

通常情况下，组织需要在执行策略之前查看云访问，以消除或限制风险。这就是为什么拥有一组离线功能来帮助您识别和评估风险状况的原因。一旦调查了威胁情况并创建了解决安全风险所需的策略，就可以将这些离线功能转换为在线解决方案，以实际执行这些策略。Gartner建议提供“两全其美”（即代理和API相结合）的解决方案，以涵盖当今组织的所有云安全使用案例。



## Forcepoint 云访问安全代理对已批准和未批准的云应用程序提供可见性和控制。

### 特点和好处

- 部署在云端安全产品的Forcepoint系列产品中，包含内置部署和云环境
- 在一个集成解决方案中包含全面的应用程序发现、治理、分析和保护
- 离线（API模式）和/或在线（代理模式）的部署选项
- 针对移动设备和端点设备的精细政策为托管和非托管手机、平板电脑和笔记本电脑提供了访问控制和数据保护
- 内置与企业目录、SIEM和MDM的集成
- 深度支持Office 365、AWS、Salesforce、Google Apps、Box、Dropbox、NetSuite、Workday、Microsoft Azure等
- 认证与身份即服务合作伙伴的互操作性：Centrify、Ping、Okta、OneLogin、SecureAuth和Microsoft
- 将组织的异常和威胁检测功能扩展到云应用程序
- IP声誉数据能够创建和实施更准确的风险缓解政策



## 云发现与治理

Forcepoint CASB通过提供有关组织特有风险因素的详细信息来扩展传统的云应用程序发现信息。例如，Forcepoint CASB提供了对呈现各种安全风险的休眠（即不活动）账户、孤立账户（如前雇员）和外部账户（如承包商）的可见性。

此外，Forcepoint还会根据行业最佳实践和法规要求对您组织的云应用安全配置进行基准测试，以便您可以更轻松地查明安全性和合规性差距并采取相应措施进行补救。

所有的云发现和治理功能都是通过云应用提供商的API启用的，这是一个非侵入性的不需要任何代理的离线流程，应用程序或日志的更改将发送到组织外的Forcepoint。

## 云计算审计与保护

Forcepoint CASB云审计和防护提供了云数据保护所需的操作智能和工具，并对用户访问进行全面控制。Forcepoint提供重要的洞察力和智慧：

- **静态数据和过境数据的丢失防护：**控制云中敏感和受管制的数据
- **用户监控：**对最终用户和管理员的实时活动进行监控和报告
- **网络威胁防护：**针对任何可疑活动提醒、阻止或要求进行身份验证的政策执行

Forcepoint CASB根据各种标准（如目标、用户或云应用程序）监控和控制敏感数据的上传、下载和共享。此外，它扫描存储在文件同步服务（如OneDrive和Box）中的公司数据，突出显示那些敏感或受监管的文件，以便您可以应用适当的策略（如发送警报）来降低风险。

Forcepoint CASB实时检查文件和内容，确保您的PII、PCI、HIPAA和其他敏感信息得到保护。管理员可以选择隔离文件，从云存储库中删除敏感文件，并通知最终用户。该文件的副本也可以添加到可信的文件夹以供进一步查看。Forcepoint CASB提供内置数据丢失防护（DLP）或具有领先DLP解决方案的基于ICAP标准的集成，以便您可以利用现有的数据保护策略。

Forcepoint CASB自动检测并阻止对云应用程序的威胁，并执行风险缓解策略。通过独特的指纹识别技术，Forcepoint CASB可以根据每个用户、部门和设备的正常使用模式快速建立详细的行为配置文件。指纹测试失败的任何访问都可以配置为实时警报、阻止或需要双因素身份验证。您还可以快速创建自定义策略，并在选定的云应用中执行这些策略。

Forcepoint CASB使您能够阻止或限制从非托管端点（如BYOD或个人设备）访问云应用程序，为通过VPN路由所有远程访问提供了经济高效的替代方案。另外，Forcepoint CASB具有内置的适配器，可以很容易地与企业目录和市场领先的SIEM解决方案集成。



## FORCEPOINT CASB – 产品功能对比

FORCEPOINT产品

功能组	功能描述	云端治理	云计算审计与保护	云安全套件
<b>应用程序 可视性和 风险评估</b>  (可在离线 / API 部署中使用)	云应用程序发现 - 利用现有的日志文件自动发现和归类所使用的云应用程序	●		●
	云应用程序风险评估 - 根据监管和行业认证和最佳实践, 对每个云应用程序的整体风险进行评估	●		●
	云应用程序使用摘要 - 包括每个云应用程序的用户数、活动、流量和典型使用小时数	●		●
	高级风险指标 —— 每个应用程序的详细云应用风险状况指标和信息	●		●
	可定制的风险指标 —— 具有可定制权重的详细云应用程序风险指标	●		●
	连续发现 —— 定期自动扫描日志文件并生成发现报告	●		●
	集中式发现面板 —— 合计式发现结果, 针对之前活动基准的当前使用情况以及使用趋势	●		●
	集成 —— 以通用事件格式生成发现数据, 以便与现有的SIEM环境集成	●		●
	应用程序目录和风险更新 —— 适当的时候自动更新云应用程序目录和风险属性的变化。	●		●
活动日志收集 —— 通过云应用程序API为用户和特权用户收集基本活动日志	●		●	
<b>账户和 数据治理</b>  (可在离线 / API 部署中使用)	数据分类 —— 对文件同步服务中存储的每个文件的敏感或规范数据 (包括共享权限) 进行编目和识别, 以确保符合PCI, SOX和HIPAA等规则	●		●
	用户管理 —— 识别休眠 (即非活动) 帐户、孤立帐户 (如前雇员) 和外部用户 (如承包商), 以降低运营成本并使相关安全威胁最小化	●		●
	APP治理 —— 根据一系列行业最佳实践和法规要求 (如PCI DSS、NIST、HIPAA、CJIS、MAS、ISO) 对您的云应用安全配置进行基准测试, 以确定其安全性和合规性差距	●		●
	集成的修复工作流程 —— 利用内置的组织工作流程, 通过Forcepoint CASB或通过与第三方票务系统集成来分配和完成风险缓解任务	●		●
<b>实时活动 监控和分析</b>  (可在在线 / 代理 部署中使用)	活动监控和分析 —— 按用户、组、位置、设备、应用程序操作等进行实时活动监控和分析		●	●
	特权用户监控 —— 对特权用户和管理员进行实时活动监控和报告		●	●
	集成 —— 直接将活动日志提供给领先的SIEM解决方案的适配器, 包括ArcSight、Splunk和Q1实验室		●	●
	企业目录集成 —— 使用现有的AD或LDAP目录基础设施来实现用户、小组和组织的报告和策略		●	●
	基于角色的管理 —— 定义用于编辑资产、策略和系统设置的管理权限		●	●
企业报告 —— 灵活的报告选项, 包括预定义报告, 可编辑和保存定制报告		●	●	



## FORCEPOINT CASB – 产品功能对比

FORCEPOINT产品

功能组	功能描述	云端治理	云计算审计与保护	云安全套件
帐户和数据管理 (可在离线 / API 部署中使用)	自动异常检测 —— 持续监控行为并检测异常活动，包括高风险的内部和外部攻击		●	●
	实时威胁预防 —— 将活动异常与危险的IP地址相关联。 <sup>1</sup> 将策略应用于应用程序内的任何应用或特定操作以警告、阻止、隔离或要求身份验证		●	●
	数据泄漏预防 - 针对超过100种文件类型和数百种符合一系列规则要求（如PCI、PII、PHI、HIPAA、SOX）的预定义数据类型的静态和实时内容检测数据分类。		●	●
	多因素认证 —— 当检测到异常或高风险活动时，基于风险的身份验证（例如，发送到用户移动设备的一次性密码）		●	●
	单一登录 —— 利用内置的SSO或第三方解决方案来访问基于SAML的应用程序		●	●
	动态提醒 —— 通过短信/电子邮件接收政策违规或活动阈值的实时通知		●	●
	移动和端点访问控制 —— 为托管和非托管设备启用独特的策略，无论是源于浏览器还是大量的移动应用程序		●	●
	基于位置的访问控制 —— 根据用户的位置或云服务的位置来限制访问		●	●
	MDM集成 —— 利用现有的MDM部署来管理端点注册和云访问		●	●
	客户政策 —— 可视化策略编辑器可以根据各种属性轻松配置定制策略		●	●
高级云架构	性能优化 —— 通过全球超过30个数据中心的世界级内容交付网络的缓存和内容优化功能，加速对云应用的访问		●	●
	统一威胁情报 —— 对企业数据库表，存储在文件共享中的文件以及存储在云应用程序中的数据等的异常和威胁的统一概览		●	●

<sup>1</sup> 可选项。将产品加载到单独购买的基础Forcepoint CASB许可证上。



**联系方式:**

[www.forcepoint.com/contact](http://www.forcepoint.com/contact)

**关于FORCEPOINT**

©2017 Forcepoint。Forcepoint和FORCEPOINT标志是Forcepoint公司的注册商标。本档中使用的所有其他商标均归其各自所有者的财产。