CLOUDVISORY：
多云计算（MULTI-CLOUD）环境的可见性、合规和治理

很多组织都必须面临管理复杂多云环境的问题。尽管云安全越来越得到保证，但是依然无法满足日益增长的云平台使用量。

FireEye Cloudvisory 提供全面的云安全解决方案，采用云原生集成技术和控件，以实现持续可见性、合规和治理，简化安全保护工作。Cloudvisory 解决了当前云安全趋势中的部分问题。

35%* 的组织坚持认为，云供应商应负责保护敏感或机密信息

云供应商的产品内置多项安全功能，但是无法满足最高安全要求。客户端组织负责保护其自身的云端数据。Cloudvisory 揭示了云供应商无法提供的关键结果，汇总来自多个云环境的数据，并突出显示安全团队需要采取的行动。

70%* 的安全团队认为，在云环境中管理隐私和数据保护合规比在组织内部的本地网络中更复杂

Cloudvisory 是唯一全面的云原生、多云计算治理解决方案，采用基于 CIS、GDPR、HIPAA、NIST、PCI 和 OpenStack Security Checklist 等安全标准和框架的最佳标准，使中心团队可更轻松、清晰地定义其责任。

56%* 的组织认为，使用云资源会增加合规风险

Cloudvisory 可持续保证多账户、多云和多操作系统环境的合规，通过对已知资产、控件和事件的配置检查，自动检测风险。Cloudvisory 合规工具可提供 1300 多项内置、自定义合规检查，且后续将添加更多。

只有 50%* 的组织定义了敏感云端信息的保护责任（尽管 48%* 的公司数据在云端存储）

Cloudvisory 通过各类模型，自动分析所有网络配置，并提出指定的活动改进建议。团队可通过 Cloudvisory 安全遥测自动测试变化，直至他们认为该变化真正可减少风险。

企业平均使用 29* 项云应用程序，增加了安全的复杂性

Cloudvisory 对云和操作系统供应商提供了广泛的支持，包括亚马逊网络服务（AWS）、微软 Azure 和谷歌云平台（GCP）。Cloudvisory 可快速安装，并与现有安全工具快速集成，所有团队都可清楚了解多云环境中的活动。

55%* 的美国组织坚信其可清楚了解云端计算应用程序、平台或基础架构服务的使用

Cloudvisory 控制面板可全面了解所有已连接基础架构的安全性。全自动、持续发现资产信息，Cloudvisory 实时维护每个服务提供商多个账户的全面资产库存，映射工作负载以发现风险。

FIREEYE CLOUDVISORY

多数企业都需要管理复杂、多云环境。将多云环境整合至集中的监控和管理解决方案，以更好地控制其当前面对的治理、合规和可见性问题。

FireEye Cloudvisory 为云安全管理控制中心，可为任何云端环境提供可见性、合规和治理信息。资产发现和合规扫描等云原生微服务支持自动端对端威胁检测，并可响应复杂的多云环境。

Cloudvisory 解决方案是唯一既可覆盖所有多云、多操作系统环境，还具有可持续特点，快速获得回报，持续提高效率和改进安全性。

若要获取更多关于 Cloudvisory 的信息，请访问 www.FireEye.com/cloudvisory

*Ponemon Institute (2019)。保护云数据 2019。Thales 云安全研究。Global Edition。