cpl.thalesgroup.com

THALES
Building a future we can all trust

全球汽车制造商提高了云端和传统系统的安全性和合规性

这家总部位于欧洲的主要汽车制造商通过多年的收购和有机增长，在世界多个国家建立了制造和销售业务。为了支持这些运营，采用云和其他平台，企业经历了一个加速数字化转型的时期。这使得成千上万的员工通过多个本地和云环境访问敏感数据的数量增加。

面对日益复杂和危险的网络安全环境，这家全球性企业希望通过其公司和子公司使用的多个平台，积极改善对其敏感数据的控制。该企业还希望继续遵守所有主要的数据保护和隐私法规，并通过多个地区市场的安全和合规审计。

挑战

该组织启动了多项举措，以提高其混合 IT 领域中高度敏感数据和应用程序的安全性。这使得相关项目侧重于以下方面：

- 保护全球子公司和总部使用 Salesforce 和 Office365 应用程序的多个实例中的敏感数据。
- 通过保护存储在包括 Windows、Linux 和 HP-UX 在内的几个传统系统上的敏感数据，改善隐私和数据安全遵从性。
- 在多个国家的数十万员工对敏感的内部资源和应用程序实施更好的访问控制。

解决方案

在多个实现过程中，Thales 帮助这家企业保护多个本地和云系统中的敏感数据，并控制总部和子公司数十万员工的访问。

Thales 通过使用 Ciphertrust 云密钥管理器 (CCKM) 解决方案的集中密钥管理生命周期，简化了 Salesforce 和 Office365 等云服务平台上的数据保护。CCKM 解决方案通过一个集中式的控制面板实现了对跨平台和租户加密密钥的完全控制，和密钥生命周期的自动化管理，并在云服务提供商自带密钥 (BYOK) 服务和汽车制造商安全团队之间实现了强有力的职责分离。

Thales Ciphertrust 透明加密与集中密钥管理的实现，保护了包括 Windows、Linux 和 HP-UX 在内的几个传统系统中的数据。Ciphertrust 透明加密使汽车制造商能够加密敏感数据，并定义细粒度的数据访问安全策略，最大限度地减少外部威胁和特权凭据滥用。

最后，利用 Thales Luna 硬件安全模块 (HSM) 作为信任根实现的基于 PKI 的访问管理和认证系统，使数十万员工能够安全地访问来自多个国家的敏感系统和应用程序。

结果

这家汽车制造商能够提高安全性，降低整个企业数据泄露的风险，并增强其整体合规状况。由集中密钥管理提供的云软件即服务环境中的安全性得到了改善，这对于允许子公司继续利用云服务，同时保持敏感的客户和企业数据的安全至关重要。

应用于传统环境中数据的细粒度安全策略集中控制增强了公司的安全态势，并加快了对诸如全球 PCI 授权和欧盟通用数据保护条例 (GDPR) 等法规的遵从。强大的基于 PKI 的访问管理和身份验证使数十万员工能够访问敏感的内部资源，而不会在每次访问时产生漏洞。

关于 Thales

您依赖能够保护您隐私的专业人员，而他们都依赖 Thales 来保护数据。当涉及到数据安全时，企业面临越来越多的决定性时刻。从建立加密策略，迁移到云端，到满足合规性要求，面临这些决策时刻时，您都可以依靠 Thales 来保障您的数字化转型。

为决策时刻提供决定性技术。

挑战:

- Salesforce 和 Office 365 中敏感数据的保护
- 改善隐私和数据安全合规态势
- 对敏感资源实施更好的访问控制

解决方案

- Ciphertrust 云密钥管理器（CCKM）
- Ciphertrust 透明加密（CTE）
- Luna 硬件安全模块（HSM）

结果：

- 通过集中密钥管理提高云 SaaS 环境中的安全性
- 加速满足细粒度安全策略的集中实现
- 通过基于 PKI 的访问管理，确保数十万员工的访问安全