THALES
Building a future we can all trust

软件与AI出海新范式

构建全球合规的软件安全及授权体系

李翔 | 高级解决方案顾问
泰雷兹圣天诺货币化

- 什么是 CRA网络弹性法案?
- CRA 核心义务与要求
- 圣天诺软件授权保护与CRA合规

Hogan Lovells

THALES

EU Cyber Resilience Act
什么是欧盟网络弹性法案

The EU Cyber Resilience Act (CRA)

- 欧盟网络安全立法的关键要素
- 欧盟商品法规框架（新立法框架）的一部分： 适用欧盟委员会的蓝色指南
- **针对投放欧盟市场的“含数字元件的产品”，明确制造商、进口商及分销商的义务**
  - ⇨ **产品安全属性**： 产品在设计、开发和生产阶段必须满足基本网络安全要求
  - ⇨ **漏洞管理流程**： 制造商必须在产品的“支持周期”内建立并遵守漏洞处理流程
- CRA合规性是获得欧盟**CE认证**和进入欧盟市场的先决条件

罚款高达500万至1500万欧元或
全球年营业额的1%-2.5%

行政命令:
如纠正措施
产品召回

解读

“包含数字元件的产品”

软件
(包括商业用途的开源软件)

硬件

以及他们的数据处理方案

软件开发商的核心义务

产品研发阶段

- 确保遵从CRA的**基本信息安全要求**
- 全产品生命周期的**风险评估**措施
- **软件供应链管理**：第三方组件（包括开源组件）
- **产品服务期限**：最低5年
- 以实体或数字形式向用户实施**信息和说明**

产品上市之前: CE 资格认证

- 根据产品类别进行的符合性评估：自我评估（**非关键**、**重要**）或由外部指定机构进行的第三方评估（**重要**、**关键**）
- 起草**欧盟符合性声明**
- 制定**技术文件**（内部）
- **粘贴**CE标志

CE

产品上市后

- 持续**监控**产品合规性并**更新文件**（至少5年）
- **漏洞管理**（测试、更新、漏洞赏金计划）
- 向ENISA/CSIRT以及用户**通知**被利用的**漏洞**和**严重网络安全事件**：在意识到漏洞/事件后24小时内发出初步通知
- 保持对用户的单点联系

Hogan Lovells

THALES
Building a future we can all trust

CRA合规生效时间表

Q3/2025 向**重要**和**关键**类别的产品施加**合规要求**

10 Dec 2024	11 June 2026	11 Sept 2026	11 Dec 2027
正式生效	**公布合格的评估机构实体**	**软件制造商的漏洞及安全事件报告义务**	**全面生效**

Q4/2025-Q1/2026
统一标准的发布

CRA 软件安全规范

Every 11 seconds there is a **ransomware attack**

Ransomware attacks alone are estimated to have cost the world roughly **€20 billion** in 2021

In 2021, **cybercriminals** launched around **10 million DDoS attacks** worldwide

基本信息安全要求 (附件 I CRA)

Part I: 数字元件产品的信息安全要求

Part II: 软件漏洞处理要求

将在**协调标准**中规定

- 软件没有**已知的可利用漏洞**（例如，软件必须更新到最新可用版本）
- 软件具有**默认安全配置**（例如，安全编码的最佳实践；利用软件保护工具）
- 处理安全漏洞的**定期（自动）安全更新**（默认启用，并提供选择退出机制）
- **访问控制**（例如身份验证、提供访问记录和报告；IAM）
- 保护（个人）数据的**机密性、完整性**和**可用性**（例如加密）
- 便捷的**永久删除**所有数据和设置的能力
- 识别和记录**漏洞**，并披露已修复的漏洞
- 软件在设计、研发和生产环节要考虑限制可能的攻击面

\+ 向ENISA/CSIRT以及用户**通知**被利用的**漏洞**和**严重网络安全事件**

适用于软件及其组件，包括开源组件

反映在**技术文件**和**软件物料清单**（SBOM）中

Hogan Lovells

THALES
Building a future we can all trust

分解CRA核心要求

CRA的要求可大致分为核心要求和边缘要求两个领域

分解前

CRA **核心**要求

- 软件在设计、研发和生产环节要考虑限制可能的攻击面
- 进行产品评估以确保其安全
- 软件不含已知的可被利用的安全漏洞
- 识别并记录已修复的安全漏洞

分解后

CRA **边缘**要求

- 为产品提供一个默认的安全配置
- 为安全性补丁升级提供一个自动更新机制
- 保护产品中涉及个人隐私的数据
- 提供便捷删除所有数据和配置的选项
- 访问控制 & 权限校验

THALES

Hogan Lovells

THALES
Building a future we can all trust

为产品提供一个默认的安全配置

如果您的：

软件默认配置不够安全，无法满足CRA要求

主流市场上，目前大多数软件都没有受到保护，可能会受到中等到低强度的攻击。 漏洞可被利用来改变产品功能的行为、暴露敏感数据或劫持其他服务。

解决方案

以安全的方式预配置并部署您的软件

部署能够抵御攻击的应用程序。利用混淆、加密和主动保护措施，最大程度上减少逆向工程和篡改应用程序代码的可能性。

泰雷兹圣天诺 如何提供帮助

圣天诺 Envelope (外壳)

- 业界公认的安全解决方案，为应用程序添加混淆、加密和主动保护措施。
- 通过阻止逆向工程尝试、利用密码学、反调试、混淆、完整性保护和其他安全技术来确保合规性。
- Envelope有助于创建安全的默认配置，交付标准安全的产品。

THALES
Sentinel®
ENVELOPE

Hogan Lovells

THALES
Building a future we can all trust

为安全性补丁升级提供一个自动更新机制

如果您：

希望为出现安全问题的软件提供更新支持

如果在您的产品内检测到漏洞，一个常见的挑战是很难识别受影响的部署并验证更新。

解决方案

提供针对性的、附加验证的自动更新

自动分发软件更新，同时启用验证和更新确认。

泰雷兹圣天诺 如何提供帮助

圣天诺 EMS & 圣天诺 Up

典型顺序：

1. **已部署产品中发现了安全问题。**
2. **利用授权历史记录来识别所有受影响的客户。**
3. **向所有受影响的客户推送强制更新。**
4. **利用EMS审计跟踪来验证客户对更新的执行情况。**
5. **维护所有未执行更新的客户的记录。**

Hogan Lovells

THALES
Building a future we can all trust

保护产品中涉及个人隐私的数据

如果您的：

产品中的个人隐私数据没有安全防护，并且能被导出

攻击者可以从正在运行的应用程序中提取应用程序数据流。静态数据也可以被提取。这会导致敏感数据暴露。

解决方案

加密保护应用程序数据

保护正在运行的应用程序的数据流以及任何静态的应用程序数据，免受提取和分析。

泰雷兹圣天诺 如何提供帮助

圣天诺 Envelope (外壳)

- 处理敏感数据的应用程序在使用时通常会将这些信息保存在内存中。
- 这些数据可以被提取并转储到文件中进行分析和操作。
- 圣天诺 Envelope 确保这些数据即使在内存中也保持加密，从而防止分析。
- 存储在边缘设备中的任何包含边缘设备中敏感数据的数据文件都可以加密，并且只能由授权的应用程序读取。

Hogan Lovells

THALES
Building a future we can all trust

访问控制 (如 身份验证, 访问日志以及报表; IAM)

如果您：

缺少控制对软件的访问，以避免未经授权的使用

未经授权的用户可以访问系统并自由使用该系统，而无需验证他们是否是合法或允许的用户。

解决方案

对所有授权用户和行为进行身份验证

确保只有经过身份验证和授权的用户和服务才允许访问特定的软件功能。记录并报告功能使用情况。

泰雷兹圣天诺 如何提供帮助

圣天诺 LDK

- **软件功能与许可证绑定。没有许可证，无法访问功能**
- **许可证根据硬件签名或用户凭据进行身份验证**
- **基于用户身份的 license 解决方案并内置IDP**
  - **圣天诺 还支持与外部IDP解决方案集成**
- **所有授权许可操作都会被记录下来，提供完整的历史记录**

THALES Sentinel® LDK

Hogan Lovells

THALES Building a future we can all trust

圣天诺 EMS 实现CRA合规 方案总结

CRA 核心要求	圣天诺 解决方案
(a) 访问控制与认证	→ 圣天诺 授权载体 (HL/SL/CL)
(b)数据机密性	→ 文件加密 DFP + 外壳加密
(c) 程序完整性	→ Envelope 防篡改 + 反调试
(d)安全更新	→ EMS 授权管理平台 + 远程更新
(e)安全日志	→ EMS 使用数据追踪
(f) 更新分发	→ EMS 许可证生命周期管理

(永久授权至少5年，或订阅模式下生命周期内)

合规效果与客户价值

- 基于许可证的精细化功能访问控制，防止非法访问
- AI模型和数据的端到端高强度加密保护
- 防止软件被逆向工程或恶意修改
- 安全补丁的自动化分发与版本追踪
- 软件使用行为的记录与监控，满足审计要求
- 精准定位受影响的边缘设备并及时推送更新

Hogan Lovells

THALES
Building a future we can all trust

THALES
Building a future we can all trust

圣天诺

AI 模型保护及授权管理

为什么AI保护如此重要?

> 声誉损失

- AI模型存在被恶意滥用的问题，这可能导致误诊、越权、不恰当的输出结果及品控投诉等，最终造成对AI及开发商的名誉损失。

> 合规罚款

- 在合规约束的相关行业，对AI的滥用将导致合规处罚，例如医疗设备行业是一个高度合规监管的行业，除了对患者的医疗安全有所考虑，合规要求也体现在了对数据隐私保护、职工安全和管理责任上。

> IP 盗窃

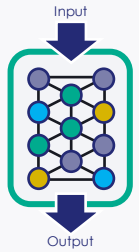
- 因为开发AI模型是一个消耗大量时间、资源的高成本项目，对AI模型进行保护将有助于开发商保护其投资,并保持竞争优势。

在不受控环境下部署AI产品将导致威胁增加

核心 | 边端

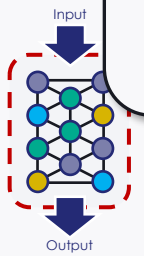
公有云

- 公有云数据中心是更安全的环境
- AI滥用发生的可能性较低



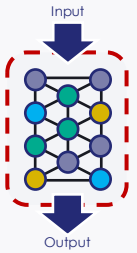
私有云

- 不受控的数据中心，安全性未知
- 无法保证访问权限
- AI滥用发生的可能性高



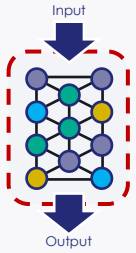
本地化部署

- 物理上可及
- 没有或欠缺对生产环境的控制
- AI滥用发生的可能性高



边端设备

- 物理上可及
- 难以管理和监控
- AI滥用发生的可能性高



部署到不受控制的环境中时针对AI的威胁

	应用程序篡改	模型篡改	模型盗窃
这是什么?	• 对支持AI的应用程序进行逆向工程，以操纵应用程序与模型之间的输入和输出。 • 为创建软件的非法副本打开大门	• 操纵人工智能模型以引入漏洞、偏见或错误	• 提取人工智能模型并在不同的解决方案中重复使用它们
风险	• 人工智能模型输出错误 • 应用程序知识产权被盗，收入损失	• AI模型输出错误	• 让竞争对手轻松获得优势
场景举例	• 错误分类图像，绕过安全系统 • 绕过验证检查并批准未经授权的交易 • 以任何形式操纵输出	• 错误分类图像，绕过安全系统 • 虚假医疗诊断 • 对IT攻击的不当反应	• 供应商窃取竞争对手的 AI 模型用于自己的解决方案，从而允许他们以低得多的成本发布类似产品。

OWASP® 这些威胁在最新的 OWASP 十大机器学习安全风险中有描述

圣天诺 AI保护组件介绍

圣天诺 Envelope

部署前

未保护的
应用程序

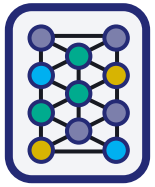
圣天诺
Envelope

部署后

受外壳保护
的应用程序

License

圣天诺 数据文件保护模块



模型文件

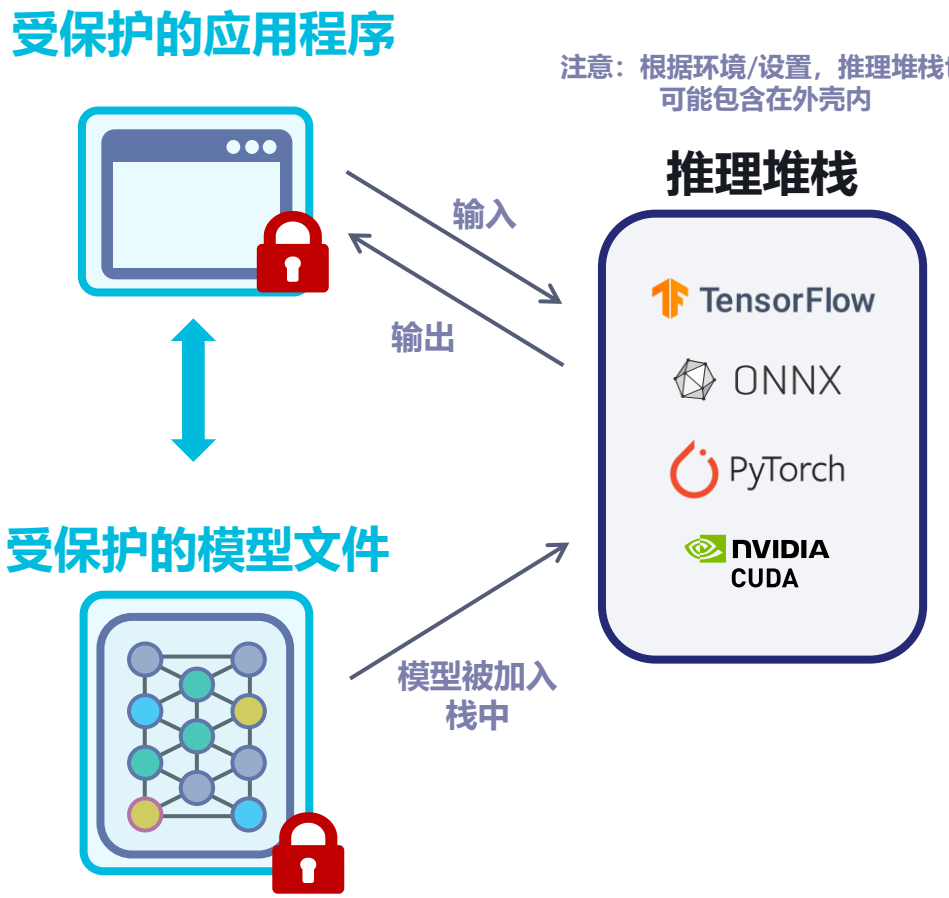
圣天诺
数据文件保护

被加密的模型文件

License

- 一旦完成保护，应用程序及模型文件将只能在有效 license 存在的前提下运行
- 信息包括了可以被允许的功能，以及任何追加的 license 策略，如到期时间和受允许的用户数量等
- 不同的应用程序和模型可套用其自身所需的不同的 license，或相同的通用license

圣天诺 解决方案总结 – 对开发商应用程序及AI模型文件的双重保护



使用 圣天诺 Envelope保护开发商应用程序

使用 圣天诺 数据文件保护 加密模型文件

> 受保护的应用程序

- 保护应用程序代码免遭反汇编和逆向工程
- 防止盗版

> 加密模型文件

- 通过阻止针对性地更改参数/权重/偏差，保护模型免受不利修改。

THALES

公司一览

83,000+
员工

68 国家
覆盖全球

€40 亿
含€ 11亿自筹资金
研发投入

€221亿
2025 销售收入

泰雷兹行业市场

商用航电

全球 #3
欧洲 #1

空管导航

全球#1
>40%

机载娱乐

全球#2

航天

50%国际空间站
增压仓

数字身份与安全

软件货币化事业部

10,000+ 全球客户在使用圣天诺软件货币化方案

2022年第三方权威市场咨询公司
Frost and Sullivan调研数据

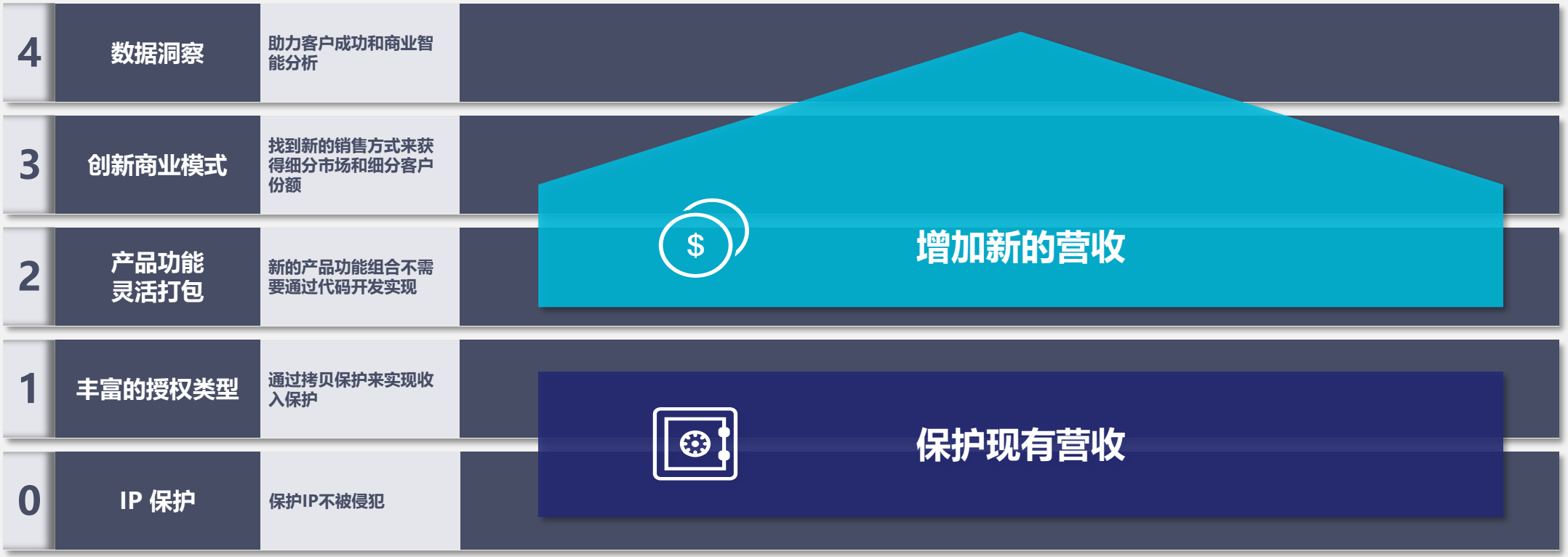
拥有 40 多年经验的全球领导者，全球市场份额： 43.4%

450+ 名安全专家，销售渠道遍布100 多个国家，为 10,000 多个组织提供解决方案。

THALES

圣天诺软件授权的五层价值

Monetization Layers



圣天诺 EMS 如何协助您的软件出海

客户体验及本地化

- 多语言本地化
- 支持自定义属性
- 一站式许可和 ESD
- 统一的户界面
- 根据 SLA 或合同承诺自动扩展

合规性符合

- GDPR 合规
- CRA 合规
- DPA 协议

数据安全存储和下载

- 每日自动备份数据快照
- 几分钟内自动恢复/故障自动切换
- 时间点数据恢复 （PITR）
- 多区域冗余自动故障切换
- 零停机更新
- 全天候全栈监控
- 每月备份/恢复混沌测试
- 设置一个或多个下载
- 将下载链接到产品
- 支持热修复交付

安全稳定的基础设施

- 高可用性
- 生成安全下载链接
- 亚马逊 Cloudfront CDN
- 数百个边缘服务器
- Google Cloud
- 符合行业标准
  - ISO 27001:2013
  - SOC 2 类型 1 和 2
  - GDPR
- 持续的漏洞和补丁管理

THALES
Building a future we can all trust

圣天诺软件授权

更多案例与介绍
随时微信端咨询

www.thalesgroup-sm.cn