nShield 即服务

轻松高效地访问加密服务

精彩亮点

- 使用托管式硬件安全模块进行云部署
- 无论在何处运行应用程序负载，始终对密钥材料保持全面掌控
- 跨多个云扩展基于云的加密和密钥管理
- 支持对基于云的工作负载执行安全代码
- 简化关键业务安全的预算制定
- 缩减维护和监控任务所需的时间

在当今快速发展的企业 IT 环境中，“云优先”是众多组织的共同战略目标。公司在本地自动托管其关键 IT 基础架构的日子已经一去不复返了。随着向云端的迁移转变，组织可以充分享受云服务提供商带来的规模、灵活性和弹性优势，同时减少维护负担，还可更精准地预测每月运维费用。如果云应用程序依赖硬件安全模块 (HSM) 以及保护作为组织加密数据信任源的加密密钥的物理设备，则这一业务转变会产生巨大压力。硬件安全模块通常位于内部数据中心，并由内部安全团队进行管理，可帮助客户满足法规或认证需求，是组织核心基础架构的重要组成部分。鉴于对企业安全团队的需求不断增长，寻找技能娴熟的安全专业人员来管理硬件安全模块是一项持续的挑战。nShield 即服务提供的功能与特性，可与本地硬件安全模块结合云服务部署的优势相媲美。客户可借此机会实现其“云优先”的目标，将这些设备的管理和维护交给 Entrust 专家。

加密即服务

“nShield 即服务”是一种基于订阅的解决方案，用于避开敏感数据，另行生成、访问和保护加密密钥材料。该解决方案使用专用的 nShield Connect 硬件安全模块，它们均已通过 FIPS 140-2 和 eIDAS (EN 419 221-5) 认证。这种云托管模型使组织可以选择在其数据中心补充或替换硬件安全模块，同时保留拥有设备的相同优势。“nShield 即服务”使企业可以更精确地计算安全预算，根据需求管理容量，减少数据中心占用空间，缩减日常维护和监视任务所花费的时间。

nShield 即服务

订阅客户与基于云的 nShield 硬件安全模块进行交互，采用与在其自有暗数据中心的设备进行交互的相同方式，但无需接收、安装和维护物理硬件。这样可缩短初次采购与使用硬件安全模块之间的等待时间，从而能够快速部署受到安全保护的应用程序。

与您的安全策略和要求保持一致

无论组织采用云优先方法来实现其加密功能，将特定服务选择性迁移到云端，又或是增强硬件安全模块能力以应对偶发性工作负载高峰，“nShield 即服务”都可以与任意安全策略完美契合。

由于“nShield 即服务”与本地 nShield 部署同样采用了独特的 Security World 架构，因此客户可以使用混合方法，将“nShield 即服务”与本地硬件安全模块结合使用。nShield Security World 是可扩展的密钥管理框架，涵盖了客户的 nShield 资产，为管理员和用户提供了一致的体验，并保证了基于订阅和本地所有设备之间的互操作性。[1]客户可以根据他们的特定环境、操作方法和安全需求，轻松高效地扩展其硬件安全模块操作。

此外，独特的 CodeSafe 安全执行功能使客户可以按需取用已扩展的安全计算能力。只有“nShield 即服务”支持客户将其安全代码执行从本地硬件安全模块无缝迁移到云端。

“nShield 即服务”的特色优势

相比其他方案，“nShield 即服务”带来以下关键优势：

- 客户可自行掌握 Security World 资源和密钥，并可在其 nShield 环境中加以使用，无论是服务形式还是内部部署
- 只有 “nShield 即服务” 可向客户提供按需控制，将其安全代码执行从本地硬件安全模块迁移和扩展到云端
- “nShield 即服务” 提供了 FIPS 140-2 3 级和 eIDAS (EN 419 221-5 安全保护轮廓) 认证的密钥安全性，这是某些云密钥保护解决方案无法实现的
- 客户可以继续将先前的业务应用程序与基于云的 nShield 硬件安全模块结合使用，并可选择使用增强的硬件安全模块容量以应对偶发性工作负载高峰
- “nShield 即服务” 可与多个云服务提供商配合使用，与之形成对比的是，其他供应硬件安全模块服务的提供商努力想要将客户困顿在他们的云环境中

注解 1. 阅读我们的 nShield Security World 白皮书，了解更多详细信息。

如需进一步了解，请访问：ENTRUST.COM/HSM

nShield 即服务

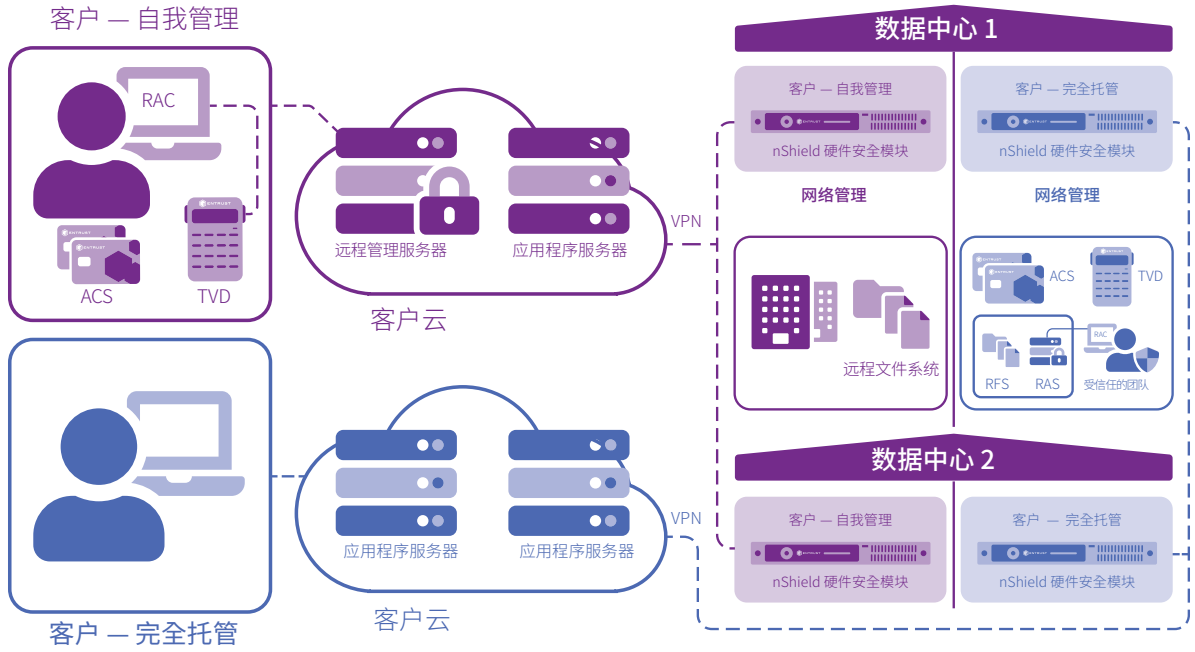
- 如果需要将数据从云服务提供商调回本地，“nShield 即服务” 即刻支持混合云部署，并可轻松进行密钥迁移
- “nShield 即服务” 为客户提供了专有的硬件安全模块服务。客户对其加密密钥享有完整控制权限，可进行双向控制，职责完全分离

选项和功能

“nShield 即服务”可实现自我管理或完全托管部署，如下图详细所述。

选项和功能

“nShield 即服务” 部署选项



KEY ACS：管理员卡片集 TVD：受信任的验证设备 RAS：远程管理服务器
RFS：远程文件系统 RAC: 远程管理客户端

“nShield 即服务”部署功能	自我管理	完全托管
客户可访问托管于安全数据中心的专用 nShield Connect 硬件	✓	✓
使用 nShield Remote Administration 工具包，您可以安全连接到基于云的 nShield 硬件管理模块并与之交互	✓	✓
维护与支持 · 服务监控 · 每年或紧急维护期间应用的预测试升级/补丁 · 全天候支持	✓	✓
对安装实例实施完整管理 · 受信任人员担任的安全官角色 – nShield Security World 创建 – 硬件安全模块注册 – 签字仪式		✓
· ISO/IEC 27001: 2013 合规策略和流程（注册证书可应要求提供） · 云安全联盟 (CSA) Security Trust Assurance and Risk (STAR) - 1 级	✓	✓
· 所有运营人员均已熟悉 BS7858（仅适用于英国数据中心）	✓	✓

如需进一步了解 Entrust nShield 硬件安全模块

HSMinfo@entrust.com
entrust.com/HSM

关于 ENTRUST CORPORATION

Entrust 支持受信任的身份、付款和数据保护，为世界的安全运转保驾护航。如今，无论是处理跨境业务、购买商品、访问电子政府服务还是登录公司网络，人们都比以往更加需要顺畅安全的体验。Entrust 提供了无与伦比的数字安全和凭证颁发解决方案，直接打通这些交互的核心。Entrust 在 150 多个国家/地区拥有 2,500 多位同事以及巨大的全球合作伙伴和客户网络，因而深受全球大多数托管组织的信任。

如需进一步了解，请访问：
entrust.com/HSM

ENTRUST

联系我们：
HSMinfo@entrust.com