

数据安全平台



产品简介

PRODUCT INTRODUCTION

“网安密+”数据安全平台是由浙江网安卫谷科技有限公司推出的，以国家商用密码（国密）体系为核心，为企业多场景数据应用提供信任、合规和安全保障的一体化解决方案。该平台构建于可弹性扩展的架构之上，通过一个集中的管理控制中心，统一管理全生命周期的密钥、安全策略和权限，并集成了多种可自由组合、即插即用的场景化安全模块。平台支持云部署、私有化（入驻式）及混合部署等多种模式，旨在帮助企业高效、低成本地构建覆盖数据全生命周期的安全防护体系，满足数字化转型中的安全与合规需求。

用户价值

USER VALUE

安全与合规

平台采用通过国家认证的商密算法和密码模块，帮助企业满足《网络安全法》、《数据安全法》、《密码法》、等保2.0、密评（GB/T 39786）等一系列国内核心安全法规与标准的要求。

统一管理，消除数据孤岛

通过集中的密钥与策略管理，确保不同信息系统加密后的数据能够互联互通，避免因采用不同加密标准而形成新的“数据孤岛”，释放数据价值。

降低成本，提升效率

一体化的平台和模块化产品降低了企业采购、集成和运维的复杂度。可视化的管理界面和集中的管控能力，显著减少了安全管理的投入和培训成本，加速安全业务上线。

灵活适配，助力转型

弹性的架构支持从传统IT到云环境、从核心业务到移动应用的广泛覆盖，为企业上云和数字化转型提供持续、一致的数据安全保护。

主要功能

MAIN FUNCTION

统一安全管理平台：提供密钥全生命周期管理、安全策略分发、权限控制、安全态势可视化及操作审计（三元分立）的核心管控能力。

应用数据加密

提供标准化API/SDK，便于现有应用系统快速集成，对服务器文件落地、数据库入库等环节的敏感数据进行国密加密。

端到端数据加密

为即时通信、音视频会议等场景提供全程商密保护，确保数据在传输过程中仅通信双方可解密。

移动端数据安全

通过安全沙箱（容器）、商密加密、水印及DLP等技术，保障移动应用及终端数据的安全。

数据库透明加密

以插件形式实现对PostgreSQL、达梦、人大金仓等数据库的存储层透明加密，无需改造应用。

动态数据脱敏/去标识化

通过API提供可配置的敏感数据动态遮盖、令牌化服务，保护测试、开发及展示场景下的数据隐私。

文件/目录/卷透明加密

在操作系统层通过安全代理，对文档、目录或磁盘卷进行实时加密与细粒度访问控制。



平台通过统一管理平台与核心场景化模块协同工作：

- ✓ 用户管理——统一管理用户身份与权限，确保数据访问可控。
- ✓ 消息服务——提供安全通信通道，保障系统间消息传输可信。
- ✓ 态势感知——实时监测安全态势，可视化呈现风险与威胁。
- ✓ 认证管理——基于国密算法实现身份强认证，确保访问真实可信。
- ✓ 策略管理——集中制定与分发安全策略，消除数据孤岛。
- ✓ 可视运维——图形化界面简化运维操作，降低管理成本。
- ✓ 服务目录——统一纳管各类安全服务模块，灵活组合即插即用。
- ✓ 审计服务——全生命周期操作审计，满足合规与溯源需求。
- ✓ 密钥管理——全生命周期管控密钥，保障加密体系核心安全。

典型用户

TYPICAL USER

政府与事业单位

需严格满足国家密评、等保要求，保护公民隐私和政务敏感数据。

金融行业

对数据安全、合规性要求极高，需保护客户账户、交易信息等核心资产。能源、交通等关键信息基础设施运营单位：受《关键信息基础设施安全保护条例》监管，需强化核心业务数据防护。

大型企业集团

拥有复杂、异构的IT系统和海量数据，亟需统一的数据安全策略来降低管理成本并防范内部风险。

正在进行数字化转型或上云的企业

聚在业务迁移和云化过程中，需要可靠的数据安全方案来应对新的风险与合规挑战。

部署方式

DEPLOYMENT



云部署(Cloud)

数据安全服务部署于中国网安的安全云上，TFE插件部署于应用系统原有计算资源中，企业无需购买任何计算资源，只需要开通服务即可。



私有化/入驻式(On-premises)

数据安全服务部署于企业内部，除密码机以硬件方式部署，其他均以软件方式部署于企业自建的计算资源上。这种方式适用于有高安全要求的封闭网络，也适用于自建私有云的场景。



混合模式(Hybrid)

企业在自有网络里建立自己的数据安全服务，服务建立后企业以租户的方式使用云（网安安全云）中的应用场景管理中心。

浙江网安卫谷科技有限公司

地址：浙江省杭州市西湖区三墩镇振华路666号名栖首座6号楼603室

网址：www.weigutech.com

邮箱：support@weigutech.com



网安卫谷