零信任解决方案

随着企业数字化转型趋势的不断加速，企业的数据资产成为了现代企业的核心价值与竞争力。传统的基于边界的网络安全架构已经无法很好的适应当前企业业务运营对数据资产的高频使用及安全需求，零信任安全理念应运而生。

零信任安全

零信任安全（ZT）旨在消除传统网络安全架构中“默认了边界内的人员、设备、信息系统是可信的”带来的风险及威胁。零信任安全架构（ZTA）通过利用不同的安全技术、策略进行编排联动，重构了以身份访问控制为基石的全新安全架构。

身份认证　身份管理　权限管理　资产管理　行为分析

传统基于边界的安全模型

基于物理网络边界构筑安全防护
假设或默认内网是安全的
主要依靠边界安全产品进行管理
主要关注未经授权的访问

零信任安全模型

基于身份的逻辑边界
认为内网与外网具有相同的风险
多产品联动实现管控
访问认证授权基于多因素且动态持续

零信任安全的优势

更强的信息安全防护能力
- 持续评估信任态势
- 动态的访问控制
- 最小化授权

更具针对性的信息资产保护
- 关注高价值资产
- 关注高访问率资产
- 关注高风险资产

更可靠的先进信息安全架构
- 适用于多种业务场景（云，物联网）
- 整合安全功能进行集中管控
- 降低运营成本

满足合规要求
- 降低合规审计成本
- 符合《网络安全法》等安全控制要求

甫瀚零信任解决方案

综合评估公司信息安全态势，设计并实施可落地的零信任转型路径

Step 1 - 现状评估
- 理解当前及未来关键业务流程
- 评估IT运营、安全控制现状
- 分析识别与零信任安全原则、合规监管要求的差距
- 基于现状评估的结果整理、开发安全控制清单

Step 2 - 零信任架构设计
- 结合安全控制清单设计零信任安全逻辑架构，包括数据安全、身份访问控制安全、终端安全等
- 确定关键零信任安全组件/产品
- 为零信任安全组件/产品提供选型标准及建议

Step 3 - 落地路径设计
- 统筹企业管理层零信任安全治理流程/战略
- 建立/更新零信任安全组织、成员职责
- 开发零信任落地路线图，通过建议分阶段实施安全项目帮助客户逐步建立落地零信任能力

Step 4 - 配套运营模型设计
- 规划建立零信任安全架构之后的配套IT运营新模式，定义关键IT运营流程中组织成员职责分工，与业务部门、分支机构间的沟通协作等

若欲了解更多或有业务咨询/合作需求，请发送邮件至：protiviti.china@protiviti.com

protiviti
Face the Future with Confidence
甫瀚