电网数据安全案例

一、背景概述

1、需求分析

电网目前的系统现状如下：

(1)主要分生产环境和测试环境(地市)两个机房，两个机房物理隔离，但目前存在某些跳板机制，从测试环境机房，可以拿到存在堡垒机的一些信息，达到获取数据的目的，是一个不可忽视的安全隐患。

(2)数据库目前将近300多套，以 Oracle（其中大部分版本为 11.0.2.0.4,小部分为12C)为主，有少量 SQL Server,DB2,MySQL,还有4套达梦数据库(其中两套用于生产环境)。

(3)服务器大约有200台，其中以 Linux、X86 居多，重要的应用服务器 AIX（小型机)为主，约50-60台，主要跑企业级的应用，如生产、营销、人力资源、资产等6+1全省集中的业务系统。

二、总体设计

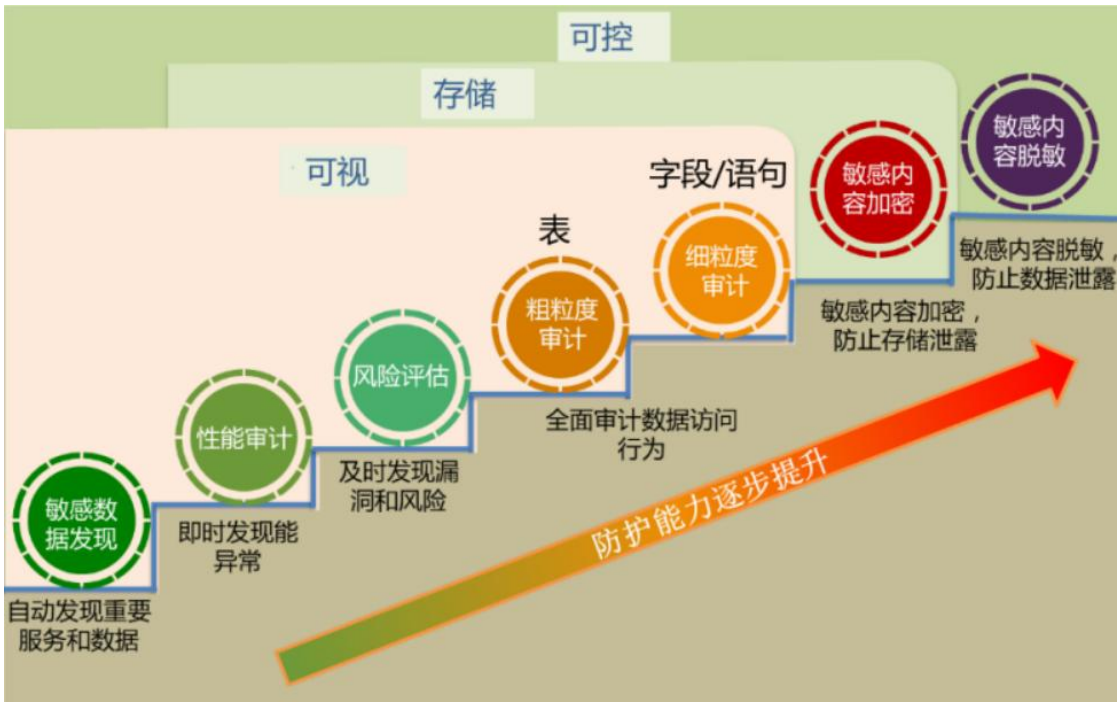
针对电网的安全需求，为了保证电网信息系统的数据安全，数达安全构建数据安全防护平台，通过可视、可控、存储安全的方式达到数据的安全防护。

1、数据可视化：无论是生产环境、测试环境，还是通过堡垒机访 问数据库，都可以实时记录数据库的访问情况及风险状况，及时发现 数据的异常活动状况和风险，并进行告警；还能针对各种异常活动提供事后追查的机制。

2、数据可控化：对敏感数据进行脱敏处理，确保运维及开发、测试人员只能看到模糊化后的数据，防止真实数据的外泄及损坏。

3、数据存储安全：针对存储大量重要数据的数据库，需要有选择 地将敏感内容进行加密存储，防止数据库系统在被入侵的情况下丢失数据，进一步增强访问控制，防止内部人员特权的滥用和盗用。

基于数据可视化，可控化及数据安全存储的需求，有针对性的对 XX 电网提供数据安全防护的解决方案，弥补现有的安全体系不足。通过敏感数据发现、性能审计、风险评估、粗细粒度审计、敏感内容 加密及脱敏相互关联，防护能力逐步提升，实现数据的可视化、存储安全及可控化。



三、方案价值

通过上述的解决方案能够有效解决该电网在生产域、测试域、堡垒机之间的实施和管理，提高数据库的安全性、机密性、稳定性以及可用性。有效满足了电网数据管理可视、可控及存储安全的需求，给客户带来的如下价值：

1、简化业务治理，提高数据安全管理能力。由于数据库系统是一个复杂的“黑盒子”软件系统，其可视化程度很低。数据库管理员很难说清在某个时刻数据被访问的情况，这对业务治理带来了很大的困难。尤其在云环境中，这种不可视化程度更加严重。我司数据安全防护解决方案通过多种手段全面监控数据的访问情况，并提供丰富的预设统计报表，以图形化的方式将数据的访问情况和风险情况可视化，进而提供访问控制能力，极大简化了业务治理，提高了数据安全管理能力；

2、维护电网的公信力。确保电网不会发生信息的泄露和不良信息的传递，提升电网在社会上的影响力和声誉。