

基于零信任架构的数据安全实践

格尔软件股份有限公司

董明富

2022 INTERNATIONAL ZERO TRUST SUMMIT
第三屆國際零信任峰會
暨首屆西塞論壇

目录

CONTENTS

01. 零信任赋能数据安全
02. 零信任数据安全方案
03. 零信任数据安全实践
04. 格尔软件公司简介

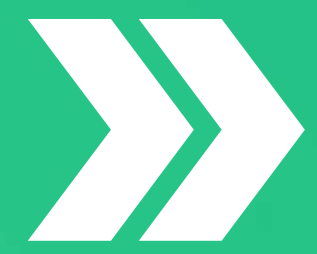


2022 INTERNATIONAL ZERO TRUST SUMMIT
第三届国际零信任峰会
暨首届西塞论坛

01. 零信任赋能数据安全

“数据安全” 民众关心的焦点

“零信任” 实现数据安全防护



数据过度收集

某打车平台过度收集1.07亿条乘客人脸信。

大规模数据泄露

据公开报道，2020年全球数据泄露的平均经济损失为**1145万美元**，国内外数据安全的形势不容乐观。

大规模数据泄露

权威机构Risk Based Security报告中显示2021年1月至2021年6月期间，**超过180亿条**敏感或机密记录被暴露，这是Risk Based Security有史以来第二高的记录。

Taxi

某打车平台数据安全事件

过度收集

违法收集



某云平台信息泄漏事件

内部泄露

出售获利

Police

某地警方破获6亿个人信息贩卖案件

数据出境

贩卖个人信息



某电信服务公司2亿用户信息被卖

出售获利

非法获取



欧盟

- 2022.3-《数据市场法案》
- 2020.11-《数据治理法案》
- 2016.4-《通用数据保护条例 (GDPR) 》
- 1995.10-《95指令》
- 1981-欧盟《个人数据自动化处理中的个人保护公约》



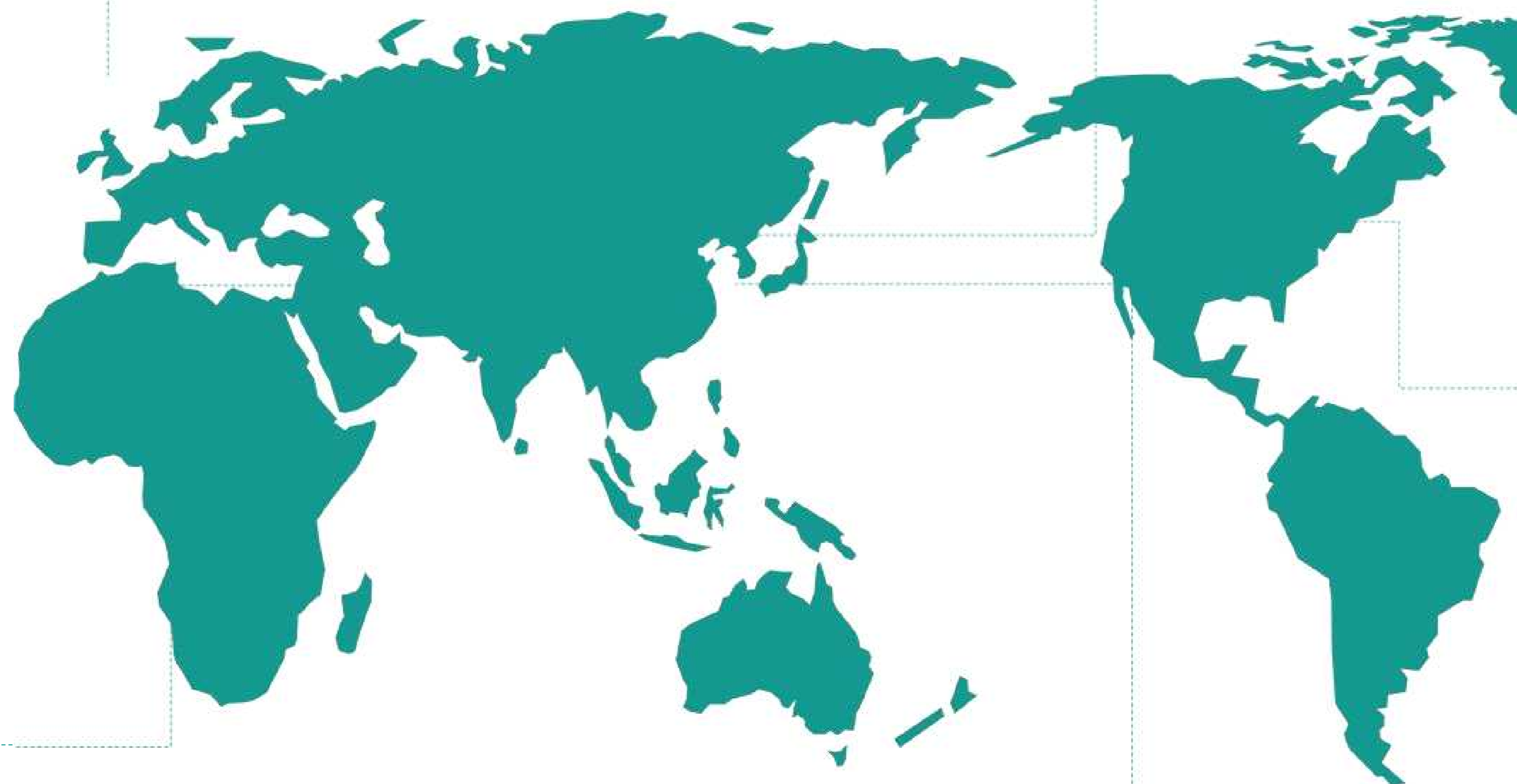
韩国

- 2011.3-《个人信息保护法》
- 2010.3-《位置信息保护和用法》
- 2009.10-《信用信息使用和保护法实施令》
- 2001.1-《信息通信网络利用促进和信息保护法》



印度

- 2018.7-《个人数据保护法案》
- 2017.11-《数据保护框架白皮书》
- 2013.7-《国家网络安全政策》
- 1999-《信息技术法》



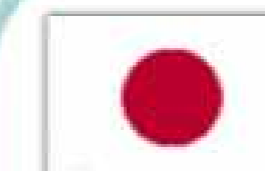
中国

- 2021.11-《中华人民共和国个人信息保护法》
- 2021.9-《中华人民共和国数据安全法》
- 2020.1-《中华人民共和国密码法》
- 2017.6-《中华人民共和国网络安全法》



美国

- 2021.8-《统一个人信息-数据保护法》
- 2021.5-《关于加强国家网络安全的行政命令》
- 2021.3-《消费者数据保护法》
- 1974.12-《隐私法案》



日本

- 2022.2-《网络安全战略》
- 2018.7-《网络安全战略（第三版）》
- 2015.9-《网络安全战略（第二版）》
- 2014.11-《网络安全基本法》
- 1988.12-《行政机关计算机处理个人信息保护法》



我国数据安全法律体系日渐完善



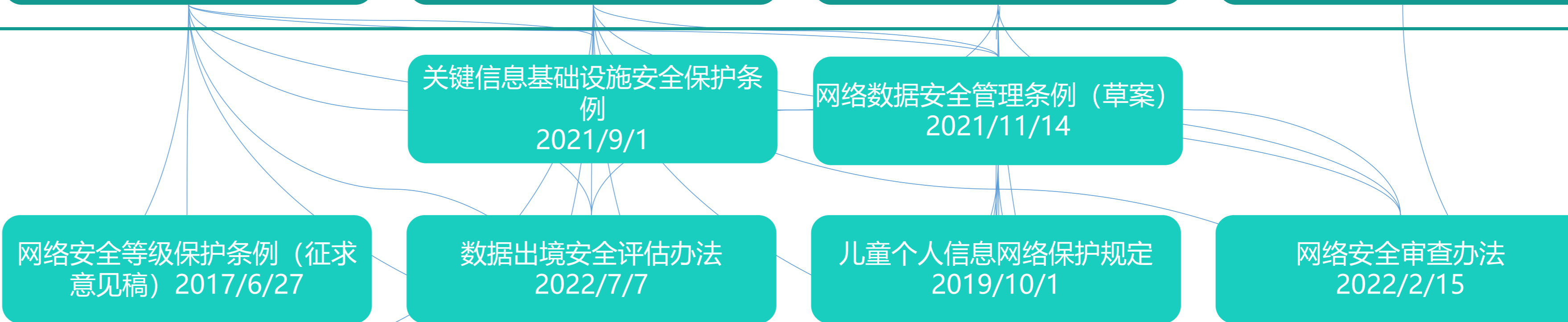
全国人民代表大会

The National People's Congress of the People's Republic of China



中华人民共和国国家互联网信息办公室

Cyberspace Administration of China



国家标准化管理委员会

Standardization administration



中华人民共和国公安部

The Ministry of Public Security of the People's Republic of China



中国银行保险监督管理委员会

China Banking and Insurance Regulatory Commission



中华人民共和国工业和信息化部

Ministry of Industry and Information Technology of the People's Republic of China





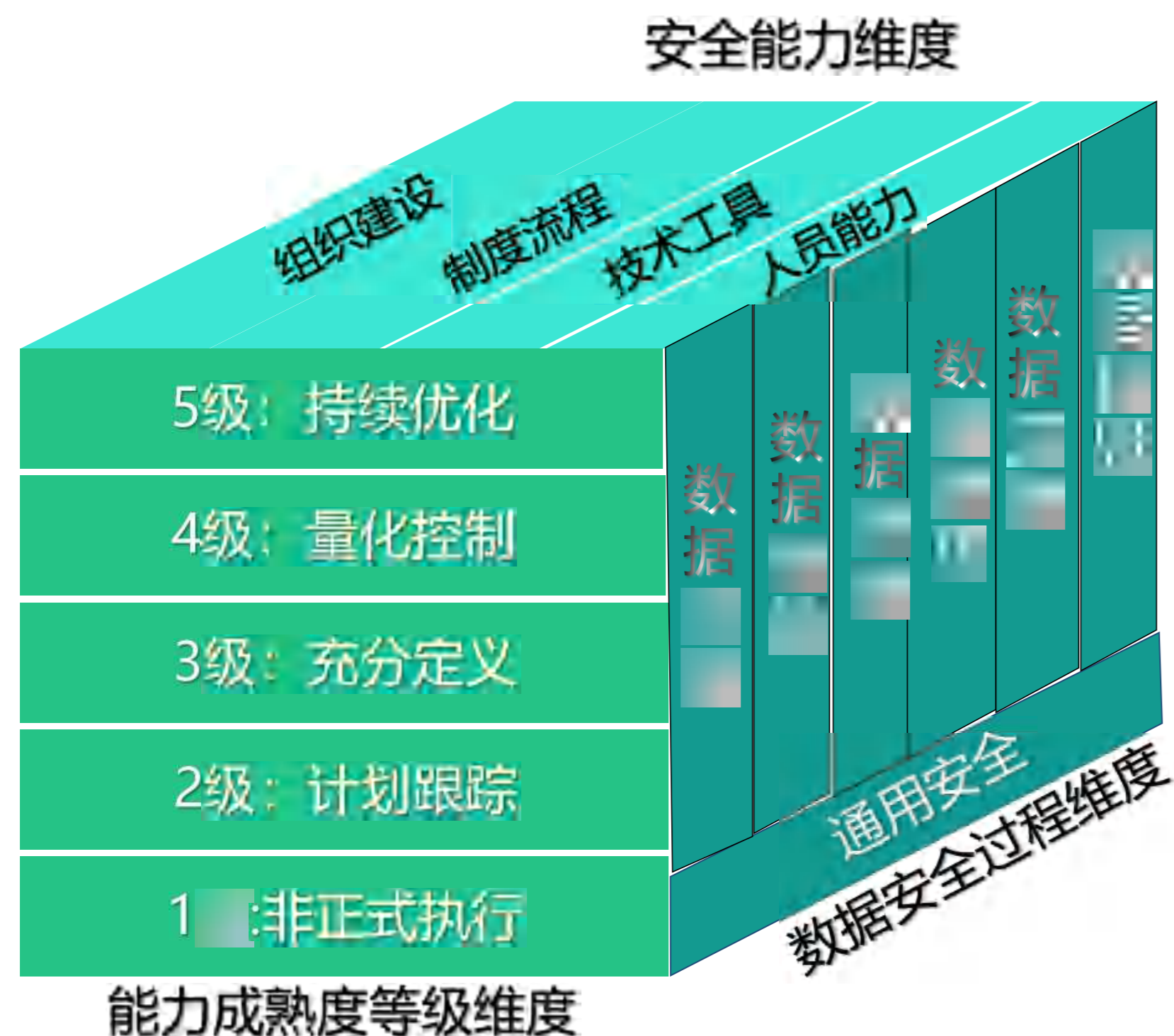
数据安全配套理论体系逐步完善

GB/T 37988 数据安全能力成熟度模型DSMM

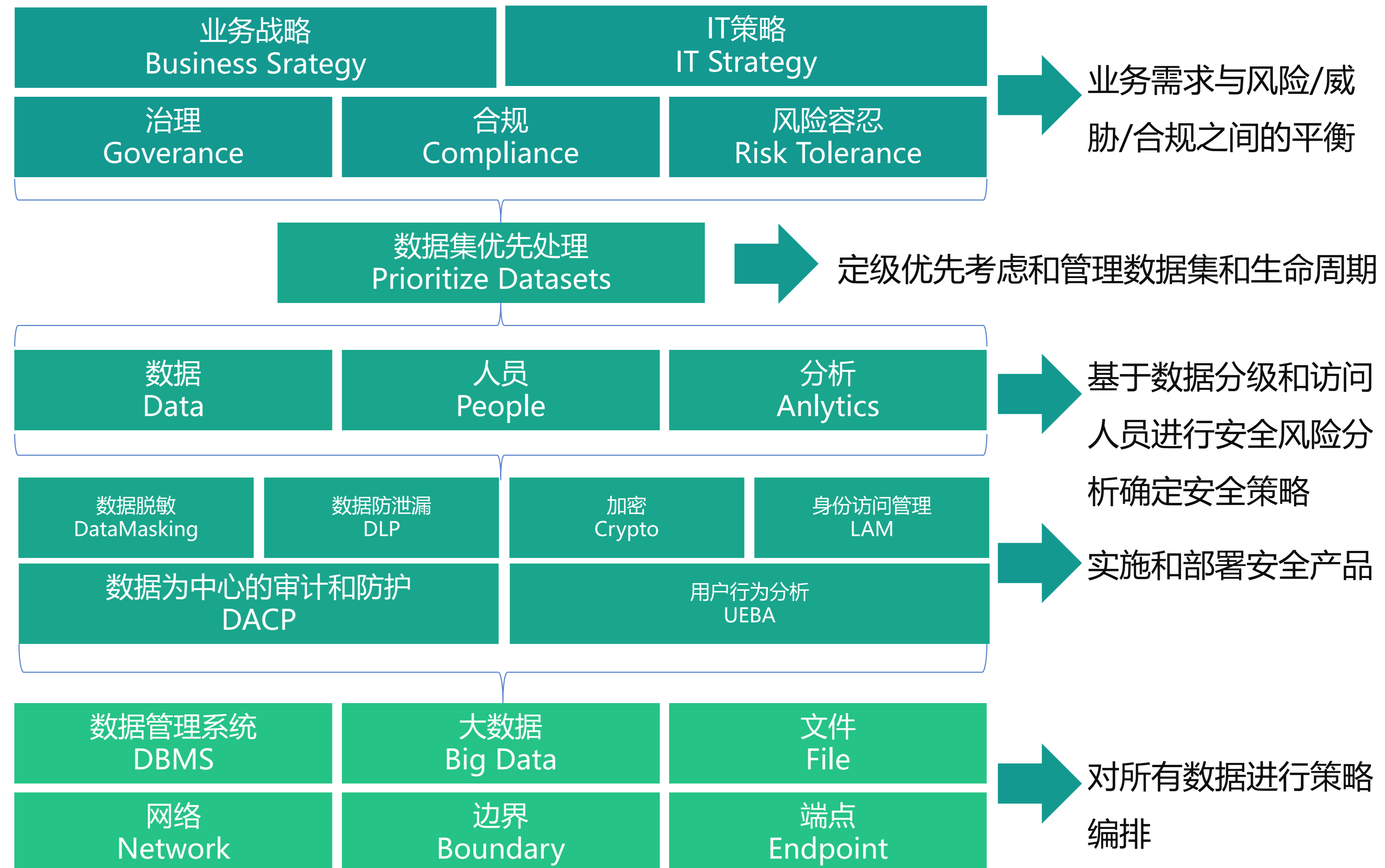
2019年8月30日正式发布

2020年3月起正式实施

4个维度 5个级别 6个阶段 30个安全域 576个基本实践



数据安全治理框架DSG



• 身份信任是前提

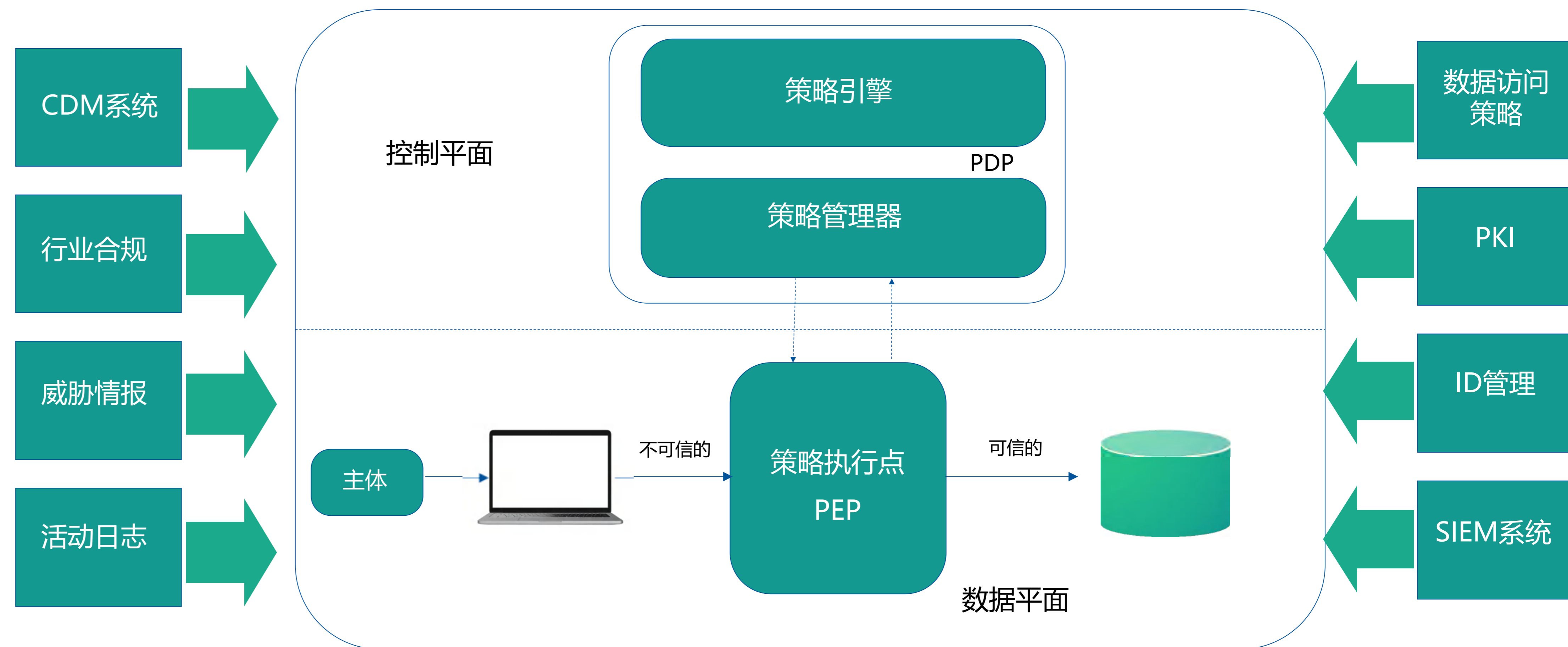
身份可信是基础和前提，默认没有信任，从零开始，结合环境、行为等多种因素持续评估

• 动态授权是手段

最小化授权是数据安全的重要措施之一，在业务授权基础上，根据环境动态、风险动态调整权限

• 整体防护是目标

数据安全是一项系统工程，需要从终端、网络、应用、数据源等多个层面进行防护，各个防护单元都要感知威胁，上报给策略管理器统一调度



2022 INTERNATIONAL ZERO TRUST SUMMIT
第三届国际零信任峰会
暨首届西塞论坛

02. 零信任数据安全方案

“数据安全” 民众关心的焦点

“零信任” 实现数据安全防护

密码为基石

密码是网络信任基石，可确保身份可信、数据机密性和完整性、行为不可否认性

身份为中心

以身份为中心，从零建立信任，授予最小权限；持续信任评估、动态访问控制

策略驱动的SDP

策略服务平台是零信任大脑，汇聚风险，收集上下文信息，持续评估，动态决策，各策略执行点执行决策结果

纵深的数据安全防护

从网络接入、终端、用户、应用、运维、API、数据访问等多个环节进行全方位对安全防护，各环节收集的安全信息回馈到策略中心，形成闭环

