



2017 中国互联网络安全大会
China Internet Security Conference

基于数据库虚拟化技术的数据安全和管理

李玉亮

数据安全部
上海上讯信息技术股份有限公司

2017 Data Breach Investigations Report

10th Edition

近日，美国最大的无线通信公司Verizon遭遇了一次大规模的数据泄露事件，由于使用了第三方NICE Systems，导致超过1.4亿的美国用户个人信息暴露在网上。

Verizon是美国最大的本地电话公司、最大的无线通信公司，在美国、欧洲、亚洲、太平洋等全球45个国家经营电信及无线业务，美国证券交易所上市。

UpGuard安全公司的网络风险调查研究员Chris Vickery发现了这一问题，他发现Verizon的这些数据存储在在一个不受保护的亚马逊S3云服务器上，任何人都可以访问并下载这些数据。

被暴露的信息中包含众多敏感信息，包括用户姓名、电话号码、账户PIN码（个人识别码）。不管是黑客还是普通用户，只要拥有这些信息就可以登录用户账户了，即便有双因素认证保护也无济于事。

	Date modified	Type	Version-ntp	
Apr01	6/8/2017 7:51 PM	File folder	Apr-2017	Unknown
Apr02	6/8/2017 7:51 PM	File folder	CF_RNVP_Fl_Flags_0201-0208_0210-0212-0214-0228-0228.ntp	40.9 MB 5/8/2017 12:07:43 AM
Apr03	6/8/2017 7:50 PM	File folder	ClsdFX_H_DATA_FEED_Jan09_Jan11.ntp	1.9 GB 3/7/2017 12:43:26 AM
Apr04	6/8/2017 8:07 PM	File folder	Feb-2017	Unknown
Apr05	6/8/2017 8:36 PM	File folder	Incoming	Unknown
Apr06	6/8/2017 8:42 PM	File folder	index.html	0 B 5/22/2017 1:45:01 PM
Apr07	6/8/2017 8:46 PM	File folder	Jan-2017	Unknown
Apr08	6/8/2017 8:49 PM	File folder	June-2017	Unknown
Apr09	6/8/2017 8:51 PM	File folder	Mar-2017	Unknown
Apr10	6/8/2017 8:52 PM	File folder	May-2017	Unknown
Apr11	6/8/2017 8:54 PM	File folder	NSP_CDR_DATA_MASKED_JAN.ntp	2.0 GB 3/8/2017 12:39:46 AM
Apr12	6/8/2017 8:56 PM	File folder	RNVP_CDR_DATA_JAN.ntp	865.3 MB 3/8/2017 12:43:57 AM
Apr13	6/8/2017 8:58 PM	File folder	Text	Unknown
Apr14	6/8/2017 9:00 PM	File folder	version.ntp	32.7 KB 3/8/2017 4:26:14 AM
Apr15	6/8/2017 9:01 PM	File folder	VoiceSessionFlnted.ntp	119.2 MB 5/17/2017 6:47:34 AM
Apr16	6/8/2017 9:02 PM	File folder	WebMobileContent.ntp	443.8 MB 5/17/2017 6:50:50 AM
Apr17	6/8/2017 9:03 PM	File folder	WebMobileContentEventNew.ntp	363.8 MB 5/17/2017 6:53:39 AM
Apr18	6/8/2017 9:11 PM	File folder		
Apr19	6/8/2017 9:28 PM	File folder		
Apr20	6/8/2017 9:48 PM	File folder		
Apr21	6/8/2017 10:10 PM	File folder		
Apr22	6/8/2017 10:23 PM	File folder		
Apr23	6/8/2017 10:44 PM	File folder		
Apr24	6/8/2017 10:49 PM	File folder		

瑞典遭遇史上最严重数据泄露事件,大量交通数据可能遭到曝光。此事在瑞典政坛掀起波澜。瑞典首相勒文日前宣布免去内政大臣安德斯·于耶曼和基础设施大臣安娜·约翰松的职务,理由是对这一交通数据泄露事件处理不当。

据瑞典电视台报道,瑞典交通管理局2015年将IT维护工作外包给IBM公司后,使得未经安全审核的外国技术人员可以获取数据库保密信息。这些信息包括瑞典全国的机动车驾驶人信息,桥梁、地铁、道路和港口等敏感信息,以及瑞典警方和军方的车辆信息。7月24日,瑞典政府承认在互联网工程服务外包中发生了大规模资料外泄。

为简化流程节省成本,瑞典交通管理局2015年在系统管理和维护工程外包过程中违规操作,将未经加密处理的交通资料库上传至外包公司位于他国的数据库。其中一家外包公司为IBM瑞典分公司,然而问题的关键在于该公司服务器实际放置在捷克,这意味着受雇于该公司的捷克电脑工程师可以轻而易举地接触到敏感数据,另一外包公司是一家塞尔维亚的通讯公司,负责维护瑞典交通管理局网络防火墙和通讯系统,也拥有查看相关数据的权限。

爆发史上最大规模数据泄露事件！瑞典政府风雨飘摇 瑞典克朗小幅下跌

🕒 2017-07-27 22:06

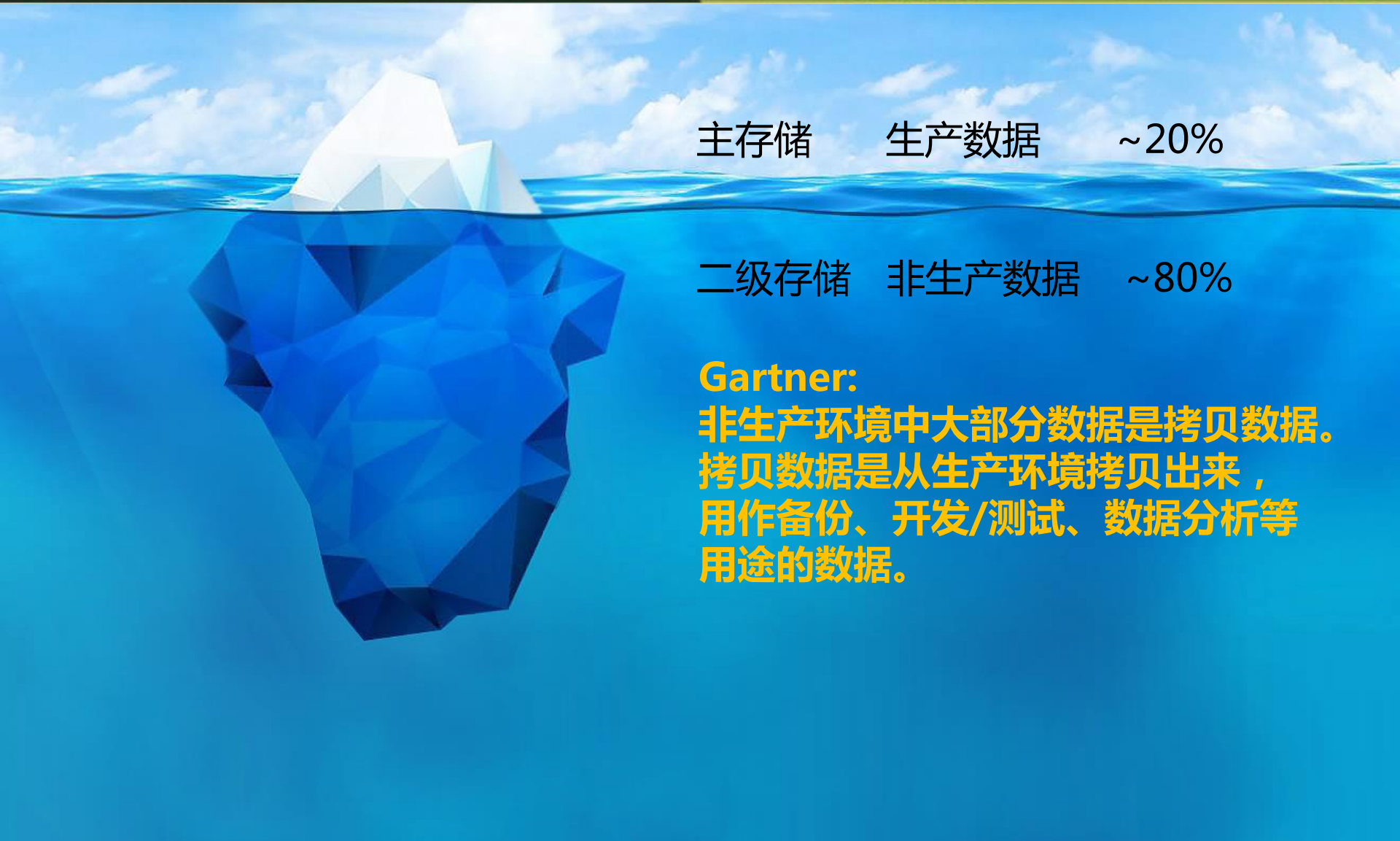
🗨 4

「摘要：这个国家正在遭遇史上最大规模数据泄露事件，政府临近崩溃边缘。首相称这是一起“灾难”，但拒绝辞职。反对党提议十天之内召集立法会议员投票，右派民粹主义政党领袖更称，要么进行新一轮选举，要么首相辞职。」

大规模交通数据泄露 瑞典两名大臣辞职

来源：羊城晚报 2017年07月28日 版次：A11G 作者：杜鹃

瑞典首相斯特凡·勒文27日接受了两名政府大臣的辞呈。这两人被指应对一起大规模交通数据泄露事件不当以及向首相瞒报相关丑闻。

An illustration of an iceberg floating in the ocean. The tip of the iceberg, which is above the water line, is white and jagged. The much larger part of the iceberg, which is submerged below the water line, is blue and also jagged. The water is a deep blue, and the sky above is light blue with white clouds.

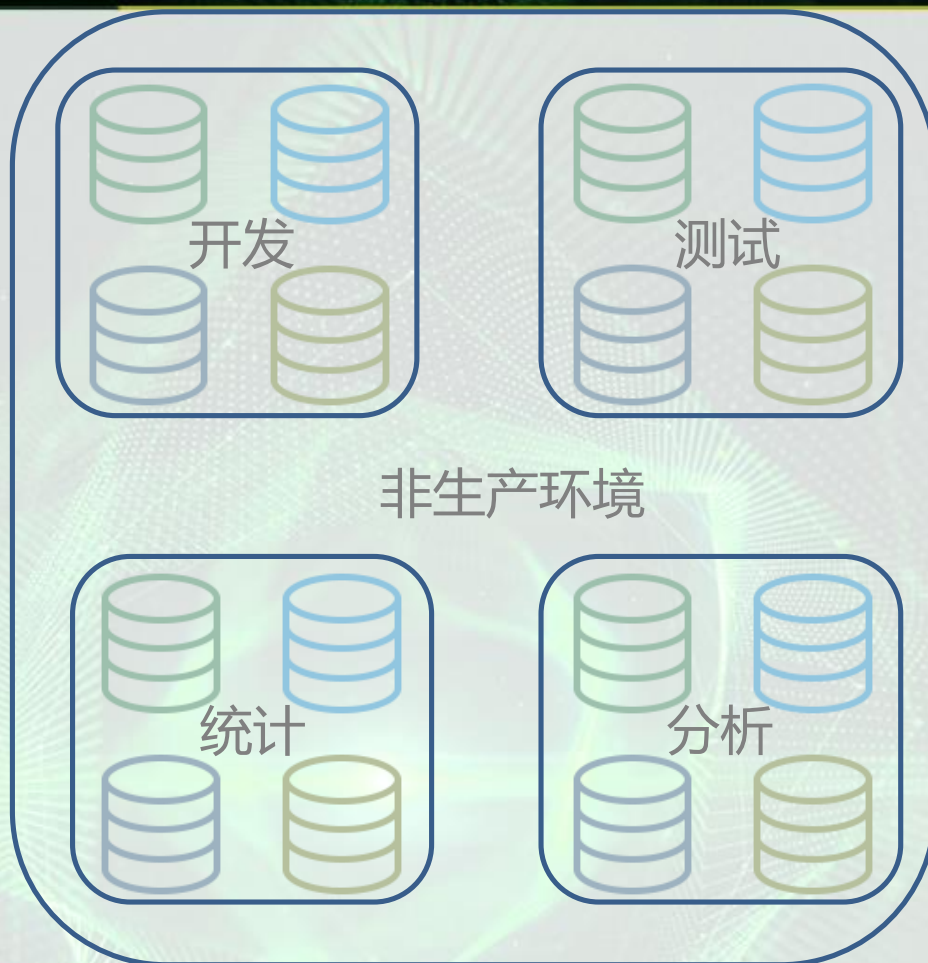
主存储 生产数据 ~20%

二级存储 非生产数据 ~80%

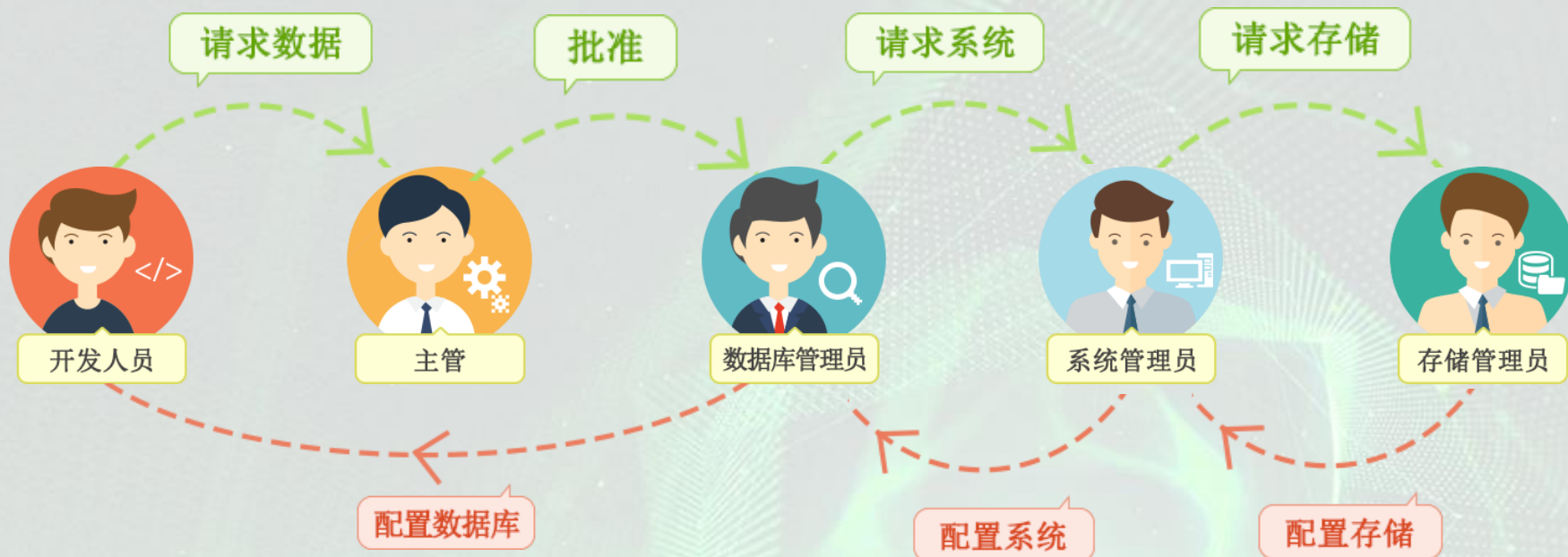
Gartner:

非生产环境中大部分数据是拷贝数据。
拷贝数据是从生产环境拷贝出来，
用作备份、开发/测试、数据分析等
用途的数据。

数据孤岛



拷贝数据的使用会产生大量的数据孤岛和巨大的存储消耗。



拷贝数据的使用流程繁琐复杂，耗费了大量的人力和时间，且无法进行集中的管理和监控，存在巨大的数据泄露风险。

数据问题



中国互联网安全大会



360互联网安全中心



2016年IDC对北美地区500家企业的调研



- 拷贝数据占用了企业**45%-60%**的存储空间。
- 到2018年，数据拷贝存储的支出将达到**500亿美元**。
- 生产环境中数据库实例的数量：**77%**的企业有超过**200个**。
- 每个生产数据库拷贝的数量：**82%**的数据库有超过**10个**。
- 拷贝数据的刷新频率：**32%**的**几天**刷新一次，**42%**的一周刷新一次。
- 刷新一次拷贝数据需要的时间：**62%**的企业超过**12小时**。
- 创建拷贝数据和脱敏的方式：**>80%**的企业自己编写脚本。

Gartner技术炒作曲线2014-2016



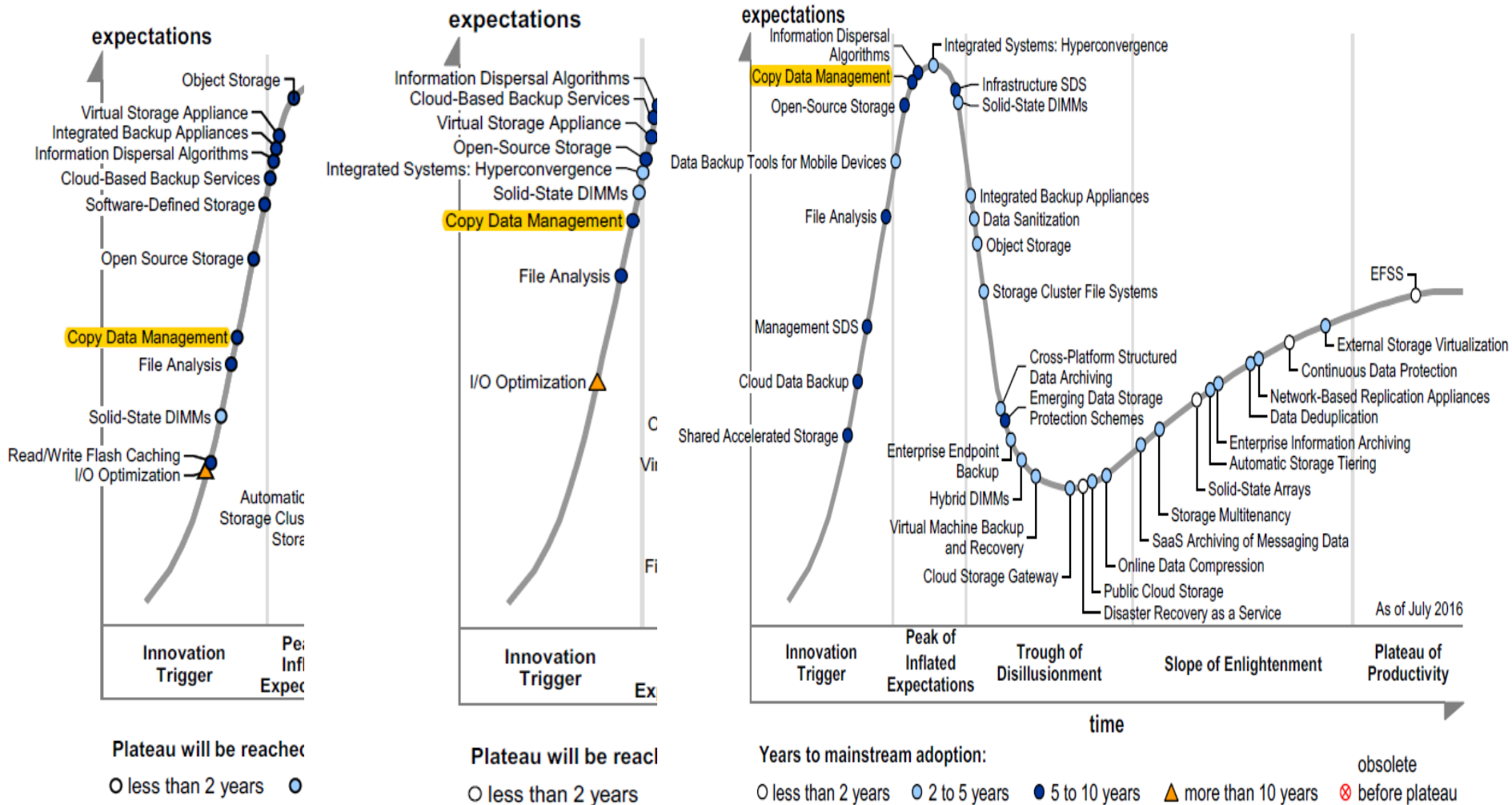
中国互联网安全大会



360互联网安全中心

Figure 1. Hype Cycle for Storage Technologies, 2016

Figure 1. Hype Cycle for Storage Technologies, 2016



数据虚拟化-存储共享



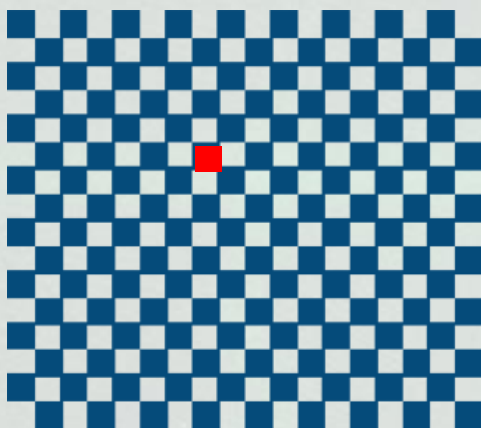
中国互联网安全大会



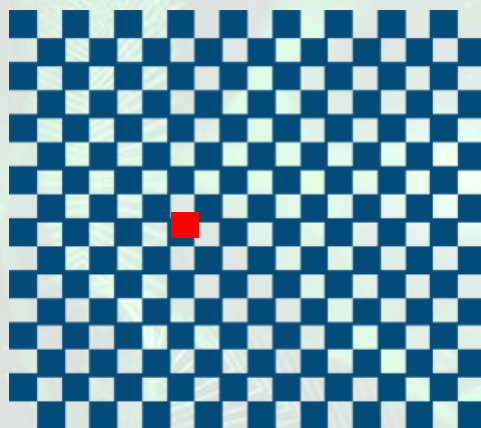
360互联网安全中心



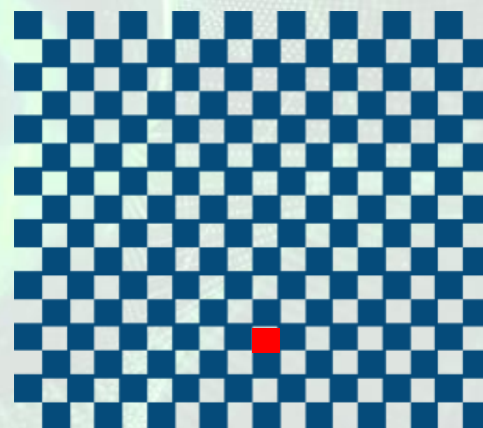
原始数据



拷贝数据1



拷贝数据2

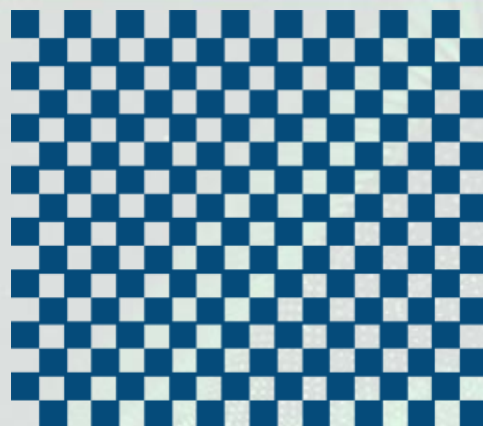


拷贝数据3

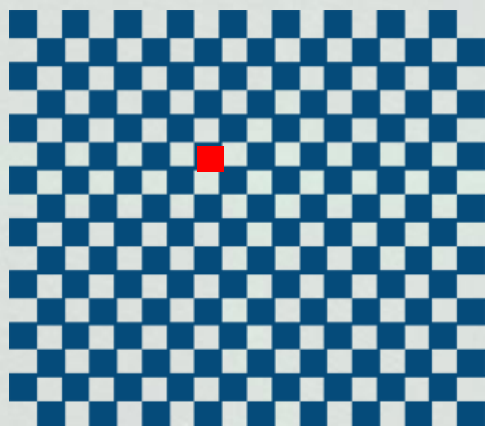
数据虚拟化-存储共享

同一份数据的拷贝之间
90%以上的数据都一样

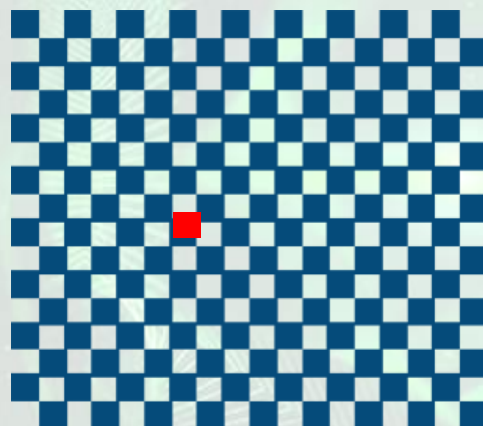
使用基于COW的文件
存储设计实现通过一份
数据拷贝支持多个独立
数据使用场景，并且能
够集中的进行访问的控
制和资源的回收。



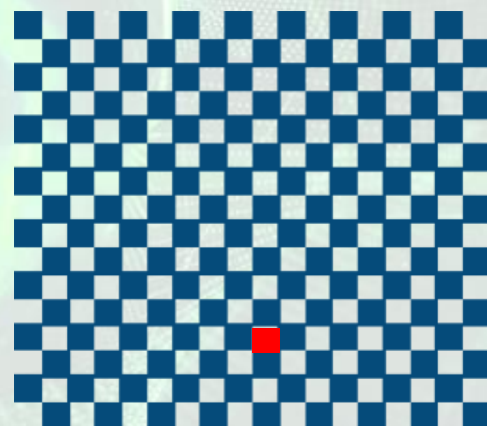
原始数据



拷贝数据1



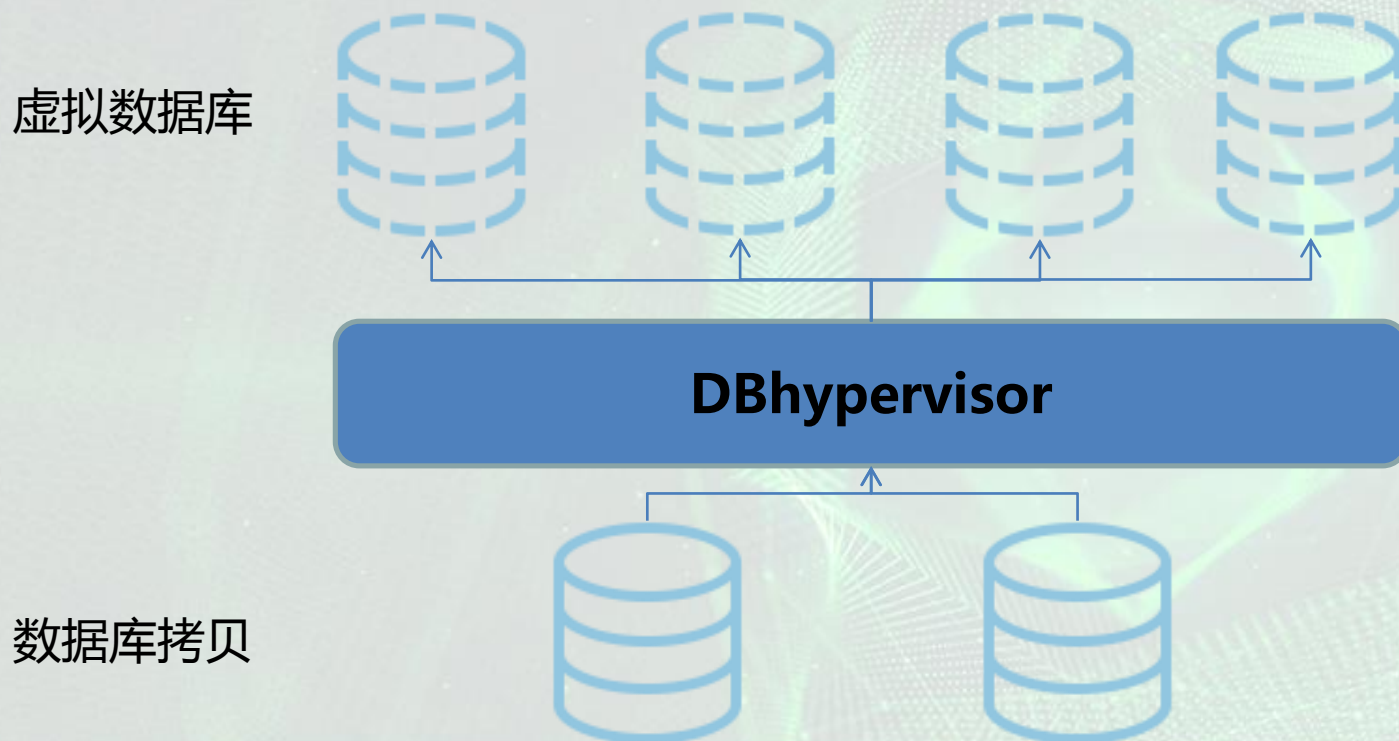
拷贝数据2



拷贝数据3

数据库虚拟化-DBhypervisor

DBhypervisor是一套数据库虚拟化管理程序，
通过一个数据库拷贝集中创建和管理多个虚拟数据库。
虚拟数据库几乎不占用额外的存储空间。
虚拟数据库之间的运行相互独立，互不干扰。
虚拟数据库的创建时间只需要几分钟。



数据库虚拟化-DBplayer

DBplayer是一个数据库虚拟化的客户端。
通过图形化的操作工具为用户提供一个自助式的数据使用体验。



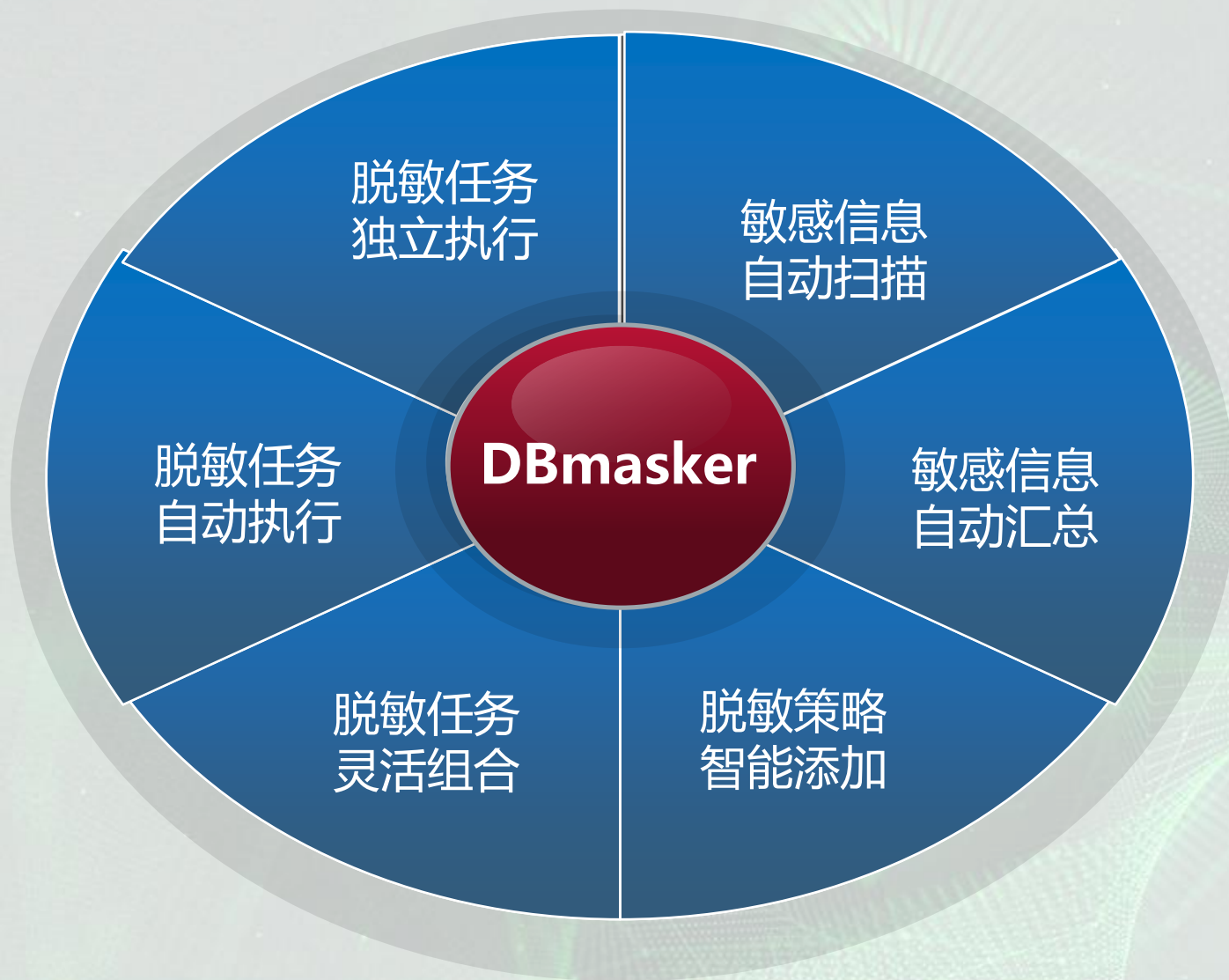
数据库虚拟化-DBmasker



中国互联网安全大会

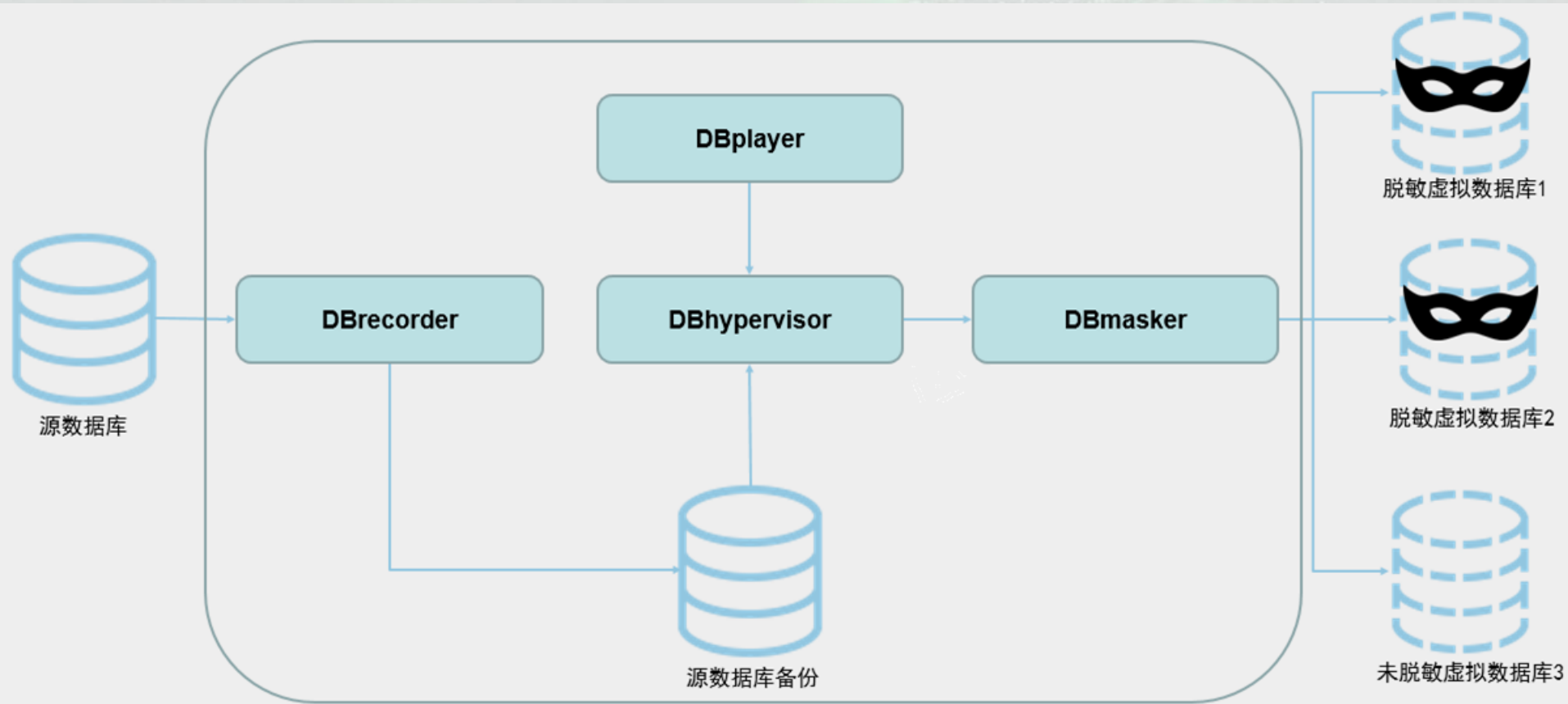


360互联网安全中心

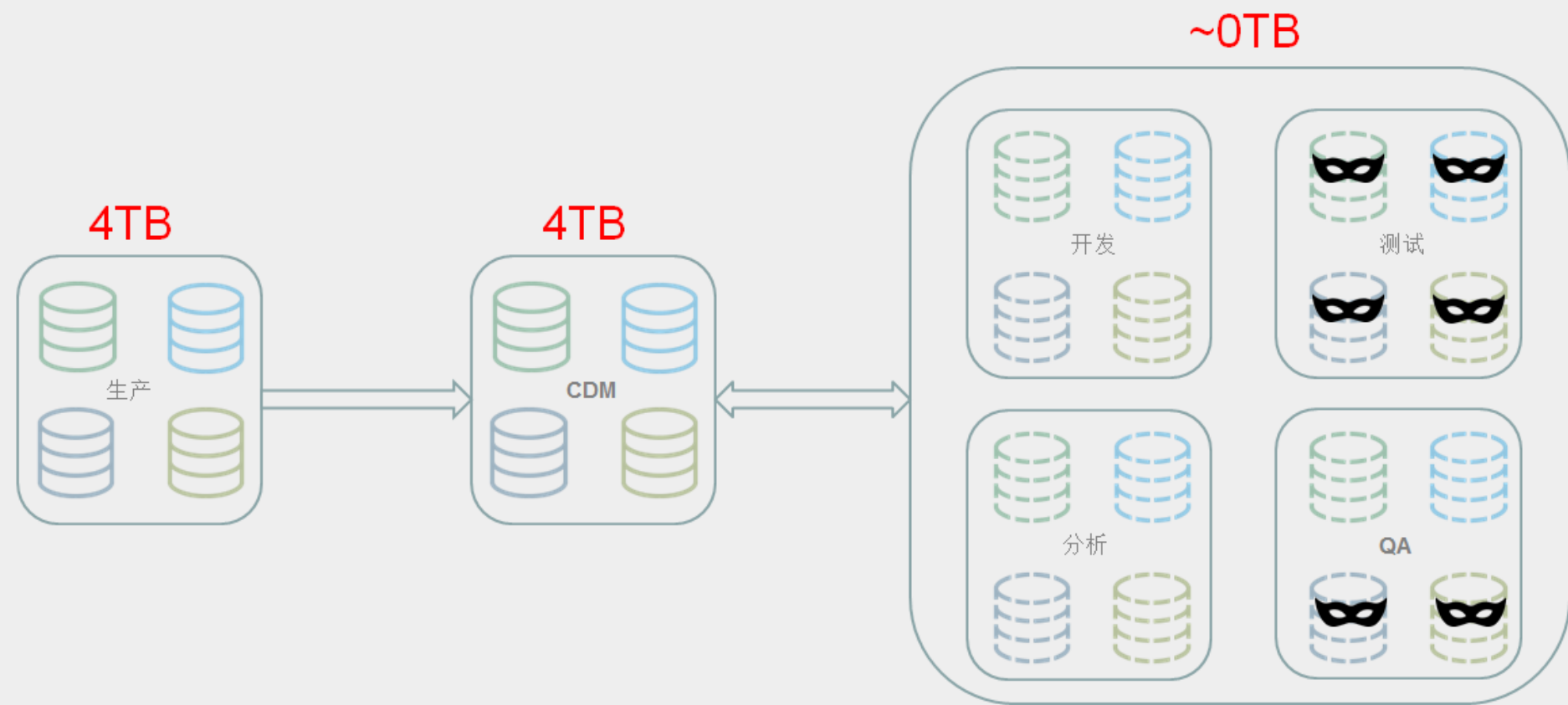


数据库虚拟化-DBrecorder

DBrecorder是一个数据同步引擎，通过首次全量备份、周期性增量备份和实时日志同步的方式将源数据库的数据同步到ADM。



数据库虚拟化-效果



总结



中国互联网安全大会



360互联网安全中心

拷贝数据管理
基于数据库虚拟化技术，
集数据管理，数据服务，数据审计于一体，
为数据管理者提供了一个集中统一的数据管理平台，
为数据使用者提供了一个简单高效的数据服务平台，
为数据审计者提供了一个安全透明的数据审计平台。

真正实现了在降低数据使用成本和提高数据
使用效率的前提下提升了数据使用的安全性。

谢 谢



中国互联网安全大会



360互联网安全中心