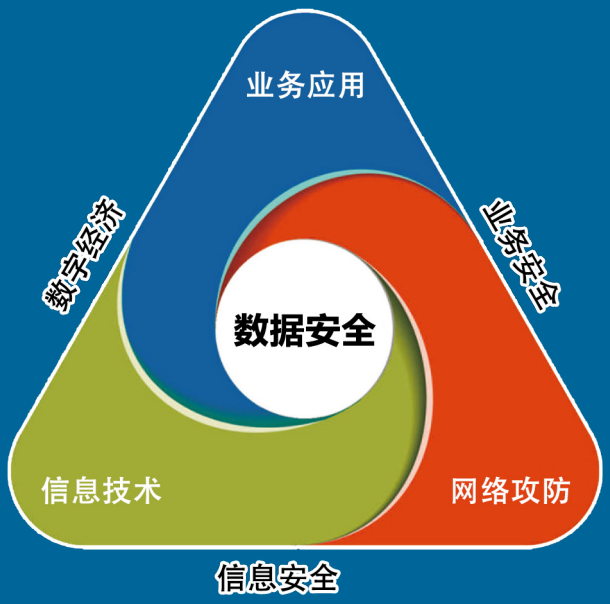
数世咨询
Digital World Consulting

数据访问安全域

能力白皮书

数世咨询
Digital World Consulting

数据访问安全域
能力白皮书



信息技术 + 业务应用 → **数字经济**

信息技术 + 网络攻防 → **信息安全**

网络攻防 + 业务应用 → **业务安全**

2020 年，数世咨询首创网络安全三元论，今年进化为“数字安全三元论”，该理论由信息技术、网络攻防、业务应用三个支点与数据安全这个核心构成，其中：

- 信息技术是 IT 基础，没有保护对象，何谈保护；
- 网络安全的伴生、服务和对抗本质，决定了它将永远的场景化、碎片化和动态化；
- 业务应用既是信息技术与网络攻防的成本来源，也是这两者最终的价值所在。

数字世界 以网络连接为基础，以数据流动释放价值，以人工智能塑造未来。
数字安全 以网络安全为基本手段，以数据安全为核心目的，支撑数字经济的健康发展和国家社会的和谐稳定。
数字世界，安全共生！

基于此，数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构、网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

主笔分析师：**刘宸宇** 综合高级分析师
分 析 团 队：**数世智库** 数字安全能力研究院
报 告 审 核：**李少鹏** 首席分析师

版权声明

目　录

目 录

前 言

数字安全时代，数据安全成为继信息安全、网络安全之后新的安全产业轴心。《数据安全法》的颁布实施纲举目张，数据安全各个细分领域开始全面落地。2021 年 12 月世界信息安全大会，数世咨询发布《中国数字安全能力图谱》，涵盖了数据资产安全，数据访问安全，数据共享安全与数据安全综合治理四大数据安全分类，这其中传统的文档安全、数据库安全，数据防泄漏以及新兴的数据应用安全与隐私计算等多个细分领域都收录在内，但仍然存在一些薄弱环节。例如，在机构用户向机构内部发起某个敏感数据（本报告中“数据”一般指用户或机构拥有的核心业务数据、商业敏感信息、知识产权信息、客户隐私信息等高价值业务数据资产）的访问请求后，数据从机构内部数据中心，通过安全的数据通路，落盘到用户终端侧，在这个过程中，机构如何落实整个访问过程的安全管控，特别是数据在用户终端侧落盘后的更进一步安全管控，目前并没有一个与之适配较强且行之有效的较好的解决方案。

据数世咨询近两年发布的“大事记”中数据泄露事件粗略统计可以看到，数据的采集、传输、存储、使用、交换、销毁等几个阶段中，发生在使用和交换阶段的数据泄漏占比呈递增趋势，发生在存储阶段的数据泄露占比呈下降趋势。此外，在众多数据泄漏事件中，内部人员、合作伙伴导致的数据泄漏事件占据了事件的多数，这其中既包括员工主动的泄密、由于失误造成的泄密，也有合作伙伴提供运维服务、业务外包和供应链等过程中发生的数据泄密。

因此，数世咨询认为，目前的数据安全正在由数据资产安全迈入数据访问和使用安全的时代——针对存储阶段的数据安全防护固然重要，其他阶段的数据安全也需要给予更多的重视；数据泄漏要面对的也不再仅仅是外部的黑客攻击，还包括内部员工、合作伙伴使用和交换数据时的数据失泄密行为。

鉴于此，数世咨询提出一个全新的细分领域——“数据访问安全域”，主

要关注的是数据访问过程中如何实现对数据的安全管控这一需求。本白皮书从场景与痛点、角色需求、技术现状、关键能力、技术要点等方面对其进行梳理与总结。本报告的内容来自于公开资料的收集、整理与调研，且主要探讨全新的数据安全细分领域，必然会有错误或纰漏，欢迎各位读者批评与指正。

团队角色及需求

对用户来说，数据访问安全通常涉及到以下 4 个角色团队：

1、业务团队 作为数据生产和消费的角色。希望通过数据挖掘出新的业务增长点，更快地进行创新并为其组织创造更多价值。这意味着数据需要在业务前端、存储节点、计算节点、数据分析节点、服务提供终端等各个节点间不断流转；

2、安全团队 希望对数据的存储、流转、访问、销毁等全过程都能够可视、可控、可查。这意味所有的数据访问请求，无论来自与外部还是内部，无论是纵向还是横向，都需要基于白名单机制进行严格的信任鉴权与控制，整个过程要具备一定程度的自动化与可视化，并定期生成安全运行报告，进而体现安全团队除了“背锅”以外的更大价值；

3、运维团队 希望安全方案尽量不改动现有的网络架构，原有的终端操作系统也不需要升级或打补丁，离线办公、远程办公、协同办公的各个业务单元都不必做出策略配置上的调整，总之就是不要动，谁动坏了谁负责；

4、法务团队 希望确保公司的安全方案遵守数据安全法等相关法律，符合等保、分保等合规要求，万一出现有意或无意的数据泄露事件，机构的法务团队能够首先从内部获取到客观有力的证明信息，避免违法违规导致的声誉受损。这意味着团队需要实现完整的数据加密和分级保护；

除了以上四个关键角色团队，最终的关键角色——老板——希望的是保业务，不出事，少花钱。这也是数据访问安全域的最主要挑战：如何在数据充分流转推动业务创新的同时，以尽量小的成本投入保证机构核心敏感数据在机构内、外的安全。

主要场景与痛点

BYOD 设备数据管控难

为了方便随时随地处理工作，企业中越来越多的员工希望可以使用私人电脑来工作，特别是针对远程办公、外包团队协作等场景，但企业难以对私人电脑终端环境的安全性进行管控，私人终端的潜在威胁可能会危及到企业业务资源，同时，企业业务敏感数据落地到私人终端后，将不受控制。

后疫情时代，普遍的在家办公场景更是如此。目前多采用 VPN+ 虚拟桌面的方式，即私人电脑通过 VPN 访问虚拟桌面从而访问企业业务数据，但这种方式对带宽的要求较高，网络的中断和卡顿严重影响工作效率和办公体验。

更重要的，由于员工在感情上普遍无法接受个人电脑中安装全局扫描类的安全产品，当需要访问财务信息、客户信息、知识产权以及其他机密信息等企业核心数据资源时，这些数据落地到员工的办公设备后，还是可能通过电子邮件、网页、即时通讯、移动存储介质、刻录、打印等途径进行传输，造成企业内部敏感数据泄露。

组织分支机构协同场景复杂

组织分支机构的数据共享和协同办公安全问题，目前多以 DLP、透明加解密、网页 Office、云盘等解决，针对研发、测试的科技类场景，还多辅以 VDI 等解决方案。这些方案，面对复杂的协同场景，各自都有一定的局限性与缺点。

例如透明加解密只能保护限定类型的文档数据，大量非文件保护的场景无法支持，研发类复杂场景无法支持；DLP 产品只在网络边界进行数据分析，无

法匹配动态变化的业务边界，无法准确控制数据的共享边界，且 DLP 需要通过设备特征和复杂的配置策略实现管理，效率与准确性较低，管理员往往为制定规则而疲于奔命。

再比如 CI/CD 场景下，有些实力较强的机构 CSO 说服领导，为员工配备了内外网双电脑隔离办公，并通过 VDI 等方案实现不同地区多团队的协同工作，然而此类方案对于具有较多分支机构的用户而言，VDI 的硬件与 License 采购建设成本、安全团队与业务、研发、运维等部门的沟通成本都比较高。

无论采用哪种方案，始终难免出现诸如数据泄密、倒卖商业情报等有损企业商誉的行为。

数据泄露审计与溯源难

第三个问题是数据泄露事件一旦发生，安全团队难以审计溯源。

首先，数据在多个部门之间流转使用，数据本身会不断衍生出新的数据，原有的数据标签与数据锚点会发生变化。其次，如何从用户对数据的正常访问行为中，甄别出恶意的行为，需要富有经验的安全管理员会同业务部门的同事一起，才有可能发现。最后，更常见的情况是，由于缺少必要的专门针对数据访问安全的审计与溯源技术工具或手段，团队 CSO 被迫需要考虑技术之外的诸多因素，业务、运维、安全、法务各个团队纠缠为一团，谁也说不清楚到底数据是从哪个环节泄露出去的。

面对上述场景中的各类风险，CSO 们要想带领安全团队避免当“背锅侠”，迫切需要构筑数据访问安全的能力。

技术现状

在提炼满足上述需求的技术要点之前，我们先梳理下现有主流的技术方案。目前与数据访问安全域相关的技术方案可以从三个方向来理解：数据安全、访问安全、终端安全。

数据安全

数据安全顾名思义主要围绕“数据”进行安全监测与防护。目前市面上的数据安全产品与解决方案，在用户侧大范围应用较多的是文档安全、数据库安全防护、数据防泄漏 DLP 等技术方案。

文档安全通过系统接口、驱动、密码及水印等技术，针对 Windows、Linux、MacOS 等不同的操作系统进行适配后，对敏感文档进行保护。如果是涉密文档，还需要对其进行分类分级、标密加密、权限管控等操作。

数据库安全防护主要围绕数据库进行，例如针对数据库资产的发现、梳理、漏洞检测、脆弱性风险评估、安全加固以及运维管控等，同时，对敏感数据的分类分级、加密解密、动态脱敏等操作也是围绕数据库展开的。

信息安全时代，数据作为固定资产，经过文档安全、数据库安全这两类防护手段，可以满足绝大部分数据安全需求，但是到了数字安全时代，数据的价值是与业务相结合，在使用中发挥出来的，因此，数据访问安全域的核心需求转变为“数据流动”中的安全，数据需要离开硬盘、数据库，来到网络或终端侧，这时，数据的完整性与安全性仅仅依靠这两种数据安全防护手段就有了明显的短板。DLP 成为了数据访问安全主要的解决方案。

DLP 以统一策略为基础，通过内容识别与分析，对机构的终端、服务器、

网络流量、应用中的各类数据提供监控与防护能力。常见 DLP 有终端 DLP、网络 DLP、应用 DLP 等：

· 终端 DLP

在机构内部的 PC、服务器等终端上运行 agent，实现对终端侧敏感数据的发现、阻断等能力；

· 网络 DLP

在关键路由节点上对机构内部的网络流量进行识别与分析，提供针对流量中数据泄露行为的可见、可查、可控能力；

· 邮件 DLP

提供邮件传输过程中的邮件数据分析、敏感数据识别审计、邮件数据脱敏、邮件审批管理、阻断策略响应等能力；

除了这三类，还有更多演变进化的 DLP 类安全产品，这里不再赘述。经过简单的梳理可以看出，针对数据访问安全域的需求，DLP 会扫描终端上存储的敏感数据，将其记录或移动至安全位置，防止企业的核心数据资产以违反安全策略规定的形式流出企业。当敏感数据离开终端的安全监控区域时，DLP 会以弹窗的方式警告用户的违规情况，当端点不在公司网络内部时，终端 DLP 会以离线数据防泄漏检测方式，继续提供安全管控。

目前采用 DLP 类解决方案的优势是，经过多年的发展与实践，厂商积累了大量的数据防泄漏策略，引入 AI 能力后，能够带来更智能的防护效果；对异常用户进行建模、对内部威胁进行分析，能够形成统一的威胁管理能力。

DLP 的不足之处在于，其采用的统一策略机制具有一定的滞后性，同时随着时间推移，策略数量积累到一定程度后会带来只增不减、难以维护等缺点；对于分支结构较多的集团类用户，需要更多的人力投入、时间投入；对于分支机构之间频繁的横向数据流动，还需要额外的数据网关进行把控，这种情况下，数据网关如何与 DLP 类产品形成统一的防护能力，同时又不影响业务连续性，

甚至如何及时跟进用户的业务发展速度，是一个同时考验业务、运维、安全运营人员的难题，需要长期投入与持续运营。

不仅如此，DLP 连同前面提到的文档安全、数据库安全，对数据的管控思路是以固定资产来看待的，即数据是被保护在“保险柜”里，数据离开一个保险柜，通过加密传输等手段放在类似于带有密码锁的“密码箱”中，然后再存入另一个“保险柜”。对于 APT 攻击者来说，保险柜和密码箱都是显而易见的攻击目标，只要有足够的耐心，盯准目标，守株待兔，“破拆”成功只是时间问题。

因此，针对数据的流通与使用环节，要保证其安全性更合理的思路是使“保险柜”或“密码箱”透明不可见，换句话说，收敛数据的潜在攻击暴露面。目前讨论较多，资本方也比较关注的技术方案是隐私计算，然而隐私计算满足的是大数据计算与数据共享过程中数据“可用但不可见”的需求，与数据访问安全域相关性不大，如何缩小数据潜在的攻击暴露面仍然需要尝试寻找更多解决方案，目前业内较为主流的技术方案是基于零信任理念的访问安全。

访问安全

新冠疫情爆发后，人们在任何设备、任何时间、任何地点对机构网络中资源的访问需求直线上升。从这个角度来说，疫情客观上进一步加速了传统的网络边界消失。传统的远程访问手段——VPN、堡垒机、远程桌面等各类产品担负起了远程办公的重任，但是对于远程的数据访问安全需求却捉襟见肘。以 VPN 举例，首先 VPN 的控制粒度较粗，要么全部都能访问，要么全部都不能访问；其次 VPN 无法控制内部访问风险，如攻击者的横向移动或东西向的恶意访问。堡垒机与远程桌面也存在着策略不灵活、管控滞后等缺陷。因此，越来越多的用户开始关注零信任理念为基础的软件定义边界（SDP）、虚拟云桌面（VDI）、远程浏览器（RBI）等实现方式。

软件定义边界（SDP）通过多维度的验证信息，对用户的身份是否可信进行证实，证实通过后，SDP 只在用户与其请求的资源间建立一条加密的安全隧

道，网络中的其他部分对该用户则不可见。 “从不信任，永远验证”使同一用户的每一次访问请求都是一次独立的验证过程，验证之后交付的资源也是相对独立的，这就使得承载核心敏感数据的 IT 资产对用户始终是透明的，减少了恶意用户扫描网络或横向移动的可能性,最终目的是将攻击面收敛到尽量小。零信任领域已经实现落地的典型代表是腾讯的 iOA 终端安全管理平台，其打造的新一代腾讯企业网NGN(New Generation Network)就使用到了SDP智能网关。

虚拟桌面基础架构（VDI）通过将服务端上的虚拟桌面传回至用户侧终端，达到保证用户侧安全的目的。VDI 能够针对不同的用户提供不同配置与应用场景的虚拟桌面，因此具备较好的个性化与灵活性。在引入零信任理念后，也能够较好的满足用户安全访问的需求。但是，目前 VDI 高时延、高成本、高复杂性等问题让大部分用户都难以承受，因此 VDI 比较适用于对高时延并不敏感且预算较为充足的机构。

远程浏览器（RBI）一定程度上避免了 VDI 的复杂性与高成本。由于浏览器的性能要求较为轻量，对用户的访问安全管控也更容易实现，管理员可以采用更为开放的互联网策略。但是由于终端侧用户的操作从桌面级变成了浏览器，对于某些专业领域应用，或是开发、设计等重度场景，RBI 的适用性范围会有些受限。这个细分领域已经有一些新锐企业在进行创新，如钛星数安，其在某国有四大行也已经实现了 RBI 的落地。

经过简单梳理可以看到，基于零信任理念的技术方案已经趋于落地，无论是互联网大厂亦或是初创企业都已经有了一些成功案例，用户根据自身不同的需求场景，选用不同的技术实现方式即可。结合本报告主题，在数据访问安全域的场景中，SDP 是一个可行的技术方案，在下文“关键能力”与“技术要点”中会再有详细论述。

终端安全

除了数据安全与访问安全，在终端侧还有一些较为成熟的技术方案，基于传统的攻防技术，帮助用户开展监测与防护。例如微软的 Windows

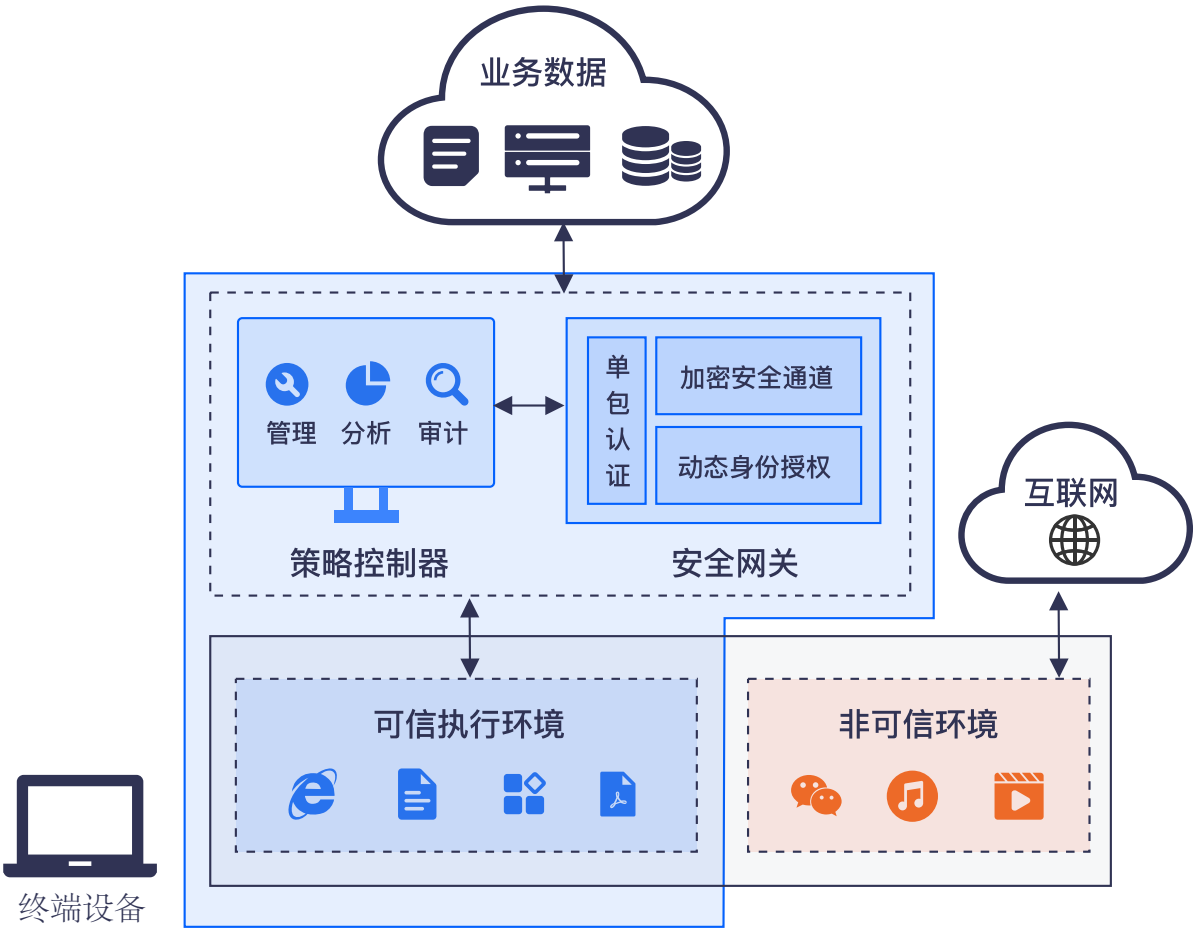
Defender、McAfee 的 Endpoint Protection 以及国内主流的终端/桌面管理、EPP/EDR、统一端点安全等技术方案，都具备较为成熟的终端安全管理能力，方案详情这里不做赘述。

这些技术方案的管控重点关注用户行为或是终端设备，管控视角侧重于攻防视角，而非数据视角。例如针对病毒、0day 漏洞、勒索软件等攻击手段有显著效果，但针对终端上的“数据访问”的管控能力相对较弱。因此很明显，不能仅仅依靠此类终端安全技术方案来满足数据访问安全域需求，还需要与前述数据安全、访问安全等方案配合使用，协助解决数据来到用户终端后“最后一公里”的安全问题。

数据访问安全域

定义

数据访问安全域是以终端安全隔离环境为核心，使用端到端的安全架构，帮助机构解决数据生产、访问、传输、使用、共享、流传等场景中的数据安全管控需求采用的数据安全技术。这里的安全域特指满足数据安全管控要求的通路、处理、存储、访问等独立空间区域。



数据访问安全域方法论

通过梳理，数世咨询认为现有的数据访问安全技术方案，其基座来源于“网络安全”，侧重于网络攻防，即通过分析数据安全链路的风险点，在数据可能的流通路径上进行埋点检测，通过数据加解密、软件策略、威胁检测等手段进行保护，传统的DLP、EDR、终端安全软件等都是基于这种思路实现。这样的实现方式，能够解决大部分数据访问的安全问题，但仍然会存在数据资产盘点不清，数据流通路径不明，数据访问管理不完整等盲区。

基于此，数世咨询认为应当以数据访问场景为脉络，建立安全、隔离的数据空间，在该空间中完成数据的访问、传输、共享、删除、追溯等全程管理，以此保护数据资产安全、共享流通以及数据访问的安全。

为保障不可信环境下的数据安全性问题，建立可以安全访问数据的防护区域，需遵从如下理论方法：

- 在不可信的终端环境里构筑起可信的执行环境，为数据提供可信的生存、活动空间。

- 确保数据访问通道的安全性，降低不可信终端与云端通讯传输过程中的安全风险。

- 围绕数据资产展开动态的攻击面发现与管理，并尽量秉持预判预防的原则对潜在的攻击面提前进行收敛。

- 将安全防护维度深入到系统底层，实现细粒度的数据访问安全区域建设。

关键能力

结合目前现有的各类技术方案，综合汇总后，我们梳理出数据访问安全域需要三个关键能力：

- 安全的数据使用终端环境
- 安全的数据传输通路
- 有机的数据治理

安全的数据使用终端环境

数据的价值在于使用，数据使用安全的关键在于数据使用环境的安全。数据使用过程中，一定会在访问用户侧落地，如前所述，仅仅以加密等“保险柜”方式进行保护是不够的，数据的访问、打开数据的应用都存在风险。因此，这里应当以“安全域”的形式建立终端数据使用的可信环境，即数据的存储、访问、应用、管理等行为都限制在安全域内。

首先，安全域环境应该是安全、高度隔离的。安全域应当对域内的网络设备、网络服务等数据交换行为加以隔离，应当具备截屏、录屏、共享屏幕、拍照、打印等防护能力，杜绝通过网络传输、外接设备等方式传出数据。总之，要能实现隔离环境的独立性、完整性以及不可伪造的唯一性。

其次，数据在安全域间的流转应该是单向、受控的。若要在安全域与非安全域之间进行文档或数据的流转，这个流转只能是单向的，非安全域中的数据可以流向安全域，反之则禁止；

第三，使用、处理数据的软件应该是可信的。对不同类型的数据，如文档、报表、网页、数据库等，应当建立受信软件列表，避免因第三方软件引入的供应链攻击。

最后，安全域环境中的用户、软件、网络等行为均应是持续监控可审计的。应当对数据访问行为中涉及到的用户行为、进程行为、网络行为、文件行为等进行持续的监控与日志记录，从而形成数据访问全流程的安全审计能力，保障数据访问过程的不可否认性。这其中重点要记录安全域中的网络访问、数据外发、数据应用、用户操作等行为日志。这部分能力对安全团队与业务、运维、法务、行政等非安全团队之间的沟通协调具有非常高的价值。

数世咨询认为，用户针对这部分能力可以重点考察供应商对终端各主流操作系统的底层技术实力。基本原则是，无论是虚拟化技术，还是操作系统的底层驱动技术，能够用相对较少的底层技术实现更多的“安全域”安全管控维度，这样对操作系统的影响最小，而相对覆盖的潜在攻击维度更多。

安全的数据传输通路

第二个关键能力是建立安全的数据传输通路，建议从两个方面重点着手。

首先是收敛潜在的攻击暴露面。潜在攻击者的所有攻击发起之前，一定要做的工作是信息收集，摸清攻击目标的所有资产信息，从中寻找最薄弱的环节，这就是攻击暴露面的概念。因此，要想收敛攻击暴露面，最有效的方式是使数据节点与数据传输通路等关键数据资产对外达到“不可见”的状态。

数世咨询建议，除了传统的资产测绘、资产管理、资产下线等方式外，基于零信任理念的 SDP 单包敲门技术是用于攻击暴露面收敛的另一个有效技术实现方式，能够以相对较小的改造成本实现关键数据资产对外的隐蔽不可见状态。

其次，加强数据通路本身的安全。可以通过加密或自定义协议等手段，防止数据流转过程中未授权用户的嗅探、劫持等潜在攻击行为，同时应用零信任

框架，对已授权用户的可能的恶意行为，在数据通路中留有判断与管控能力，即对其能够访问的资源进行精细化管理。例如对 IP 地址、网段、域名、端口等用户拟访问的资源通过白名单或系统策略等机制进行最小化、动态访问管控。

要实现这一能力，除了目前较为成熟的加解密外，数世咨询认为，还可以重点从“协议”入手。即在条件允许的情况下，通过网络协议的定制化，将通用协议修改为潜在攻击者难以识别的自定义协议。当然，前提是不能影响用户的正常业务，因此，具体的定制化改造，特别是对用户已有的业务 API 数据接口、VPN 身份认证接口等，要综合评估改造成本与改造收益之间的平衡。

有机的数据治理

首先，不应受限于数据的类型、种类、数量、大小、业务软件等，数据访问安全域要能广泛覆盖如文本、文档、图像、音视频、代码、图纸以及未知文件类型等各种各样的数据类型。

其次，数据访问安全域要具备数据分级治理的能力，即针对不同类型的数据，采取不同的治理策略。例如对于核心敏感数据，限定允许访问数据的应用、用户、来源等，防止数据的越权、越界访问；又如对高风险数据，如邮件附件或安全性未知的网站、文档、软件等，要对这些高风险数据的活动边界进行强隔离，阻止潜在的安全威胁扩散。

第三，基于以上两点，数据的治理要以有机为目标，做到可更新、可持续。从数据的采集、创建开始，数据的元信息（各类标签、管控策略等）要在数据流动过程中，一直跟随着数据一起流动、更新，并进一步实现对数据的复制、修改、删减等操作能追溯到数据的起始来源和流传路径，以此作为数据访问控制策略、交换策略、审计策略的重要参数与决策依据。

技术要点

基于上述各个能力，数世咨询认为 “数据访问安全域” 主要用到以下几个技术要点：

- 虚拟化技术
- 终端侧攻防对抗技术
- 零信任访问技术
- 数据标签技术

虚拟化技术

通过对文件系统、网络设备、进程模块等系统环境的虚拟化，在用户终端上构建出一个独立的安全区域。安全区域与非安全区域的文档、数据、注册表、内存、进程对象、网络对象、PNP 设备等各自均独立、完整运行。

这里的“虚拟化”应当在操作系统内核级实现，且具备较高质量的产品化与工程化，如此才能保证虚拟出的安全区域中，应用的安装、使用、分发等操作安全、独立、顺畅，既不影响业务应用的运转与核心数据的流转，又能保证数据访问在终端侧的安全隔离与管控。

终端侧攻防对抗技术

一是系统底层攻防。通过对底层驱动、进程行为、系统状态、用户操作等持续的安全监控，杜绝目录篡改、恶意驱动、非法模块、进程注入等针对系统

的攻击行为，避免恶意攻击者对安全域的破坏与逃逸。

二是反嗅探。这一点与数据通路防护能力相对应，即在用户终端侧，通过重新编写的网络通信协议栈规避抓包与监听，如有可能，避免使用虚拟网卡，防止终端侧与 SDP 网关之间的通信流量被嗅探攻击。

三是硬件数据防篡改。在数据加解密、密钥管理、策略判断、安全域完整性保障等关键环节，结合可信执行环境（Trusted Execution Environment - TEE）等硬件可信计算技术，实现硬件级别的数据抗篡改能力。

零信任访问技术

即基于 SDP 的零信任访问技术。SPA 单包敲门机制保证了所有的 DDoS 攻击与扫描探测行为都被屏蔽在 SDP 网关之外，实现了所有资产对外零可见。默认关闭所有端口，仅在用户认证通过并授权后，动态分配业务开放端口，并在所请求资源与用户终端间实时建立加密连接，这保证了用户的每次连接都是独立的。

如前所述，SDP 是构建攻击暴露面收敛能力的主要技术手段。值得一提的是，SDP 并不是数据访问安全域所必须的，端到端的安全是主要目的，其他能够达到这一目的要求的技术均可采用。

数据标签技术

数据在不断的流转过程中，经过修改、共享、复制、再分发等多个流程后，依旧可追溯其数据来源和流转路径，这里的难点是如何在数据量不断增大或业务迭代带来新的数据类型后，数据标签在及时更新的同时，保持数据分类、分级、分代的准确性，进而保证数据治理的效果不出现明显波动，不影响数据访问安全的控制策略、交换策略与审计策略。

目前行业内主要的技术实现方式是结合行业属性，将行业特征转化为“行

业标签体系”，应用于数据标签；或者根据数据的访问关系，提炼出数据的访问链路，进而一定程度上实现数据标签的自动化补足与更新。但目前，这两种方式还都无法实现完全的基于 AI 的智能数据标签，仍然是“人工”为主要驱动的“智能”，因此相比数据标签“技术”，数据治理其实更多也是一个管理问题。

说句题外话，数据治理与数据安全的结合，“数据治理安全”与“数据安全治理”的区别等内容，数世咨询另有相关报告《数据治理安全能力白皮书》进行讨论，读者可以持续关注。

数据访问安全域代表企业

结合前述几项核心能力与技术要点，数世咨询通过公开资料的收集、整理与走访调研，认为以下代表企业是符合数据访问安全域这一新的细分领域的，供读者参考。

Citrix

Citrix 成立于 1989 年，先后通过与微软、ExpertCity 、Xen、Cloud.com、Google 等公司的合作或资本运作，已经在多用户远程访问服务器与桌面虚拟化市场这个领域深耕了 30 多年，国内用户对这家公司的了解大部分是在 2007 年收购 Xen 之后。 2018 年，在坚定地向云运营模式转变之后，现在的 Citrix，以“将人、事和公司安全地联系起来”作为使命，提供的是“随时随地在任何设备的所有应用程序中”都能使用的 DaaS 桌面即服务产品。

对用户来说，Citrix 提供的“高性能数字工作空间”能够让员工在远程办公的同时，放心可控的访问其核心数据。由于采用“XaaS”的交付方式，因此相比使用其他同类产品，用户能够省去较多的管理难度。在这背后，Citrix 采用的是虚拟化、VDI、零信任访问以及统一端点管理等多个技术实现方式，以保证用户的数据访问安全。

除了微软和 Google 之外， Citrix 还与 AWS、Cisco、HP、Intel、Okta、SAP 等知名企业组成了战略合作关系，与这些公司的产品也有深入的整合。因此，对于大型机构类用户来说，Citrix 的产品具有较好的适用性，相应的，成本也会较高一些。

Vmware

作为虚拟化技术的全球领导者，Vmware 在数据访问安全域领域的 VMware Workspace ONE 产品为用户提供的是具备统一端点管理、虚拟桌面以及零信任访问控制的数字化工作空间。

由于是基于统一端点管理（UEM）技术构建，Vmware 的方案能够在多种类型的终端设备上运行。虚拟桌面与零信任访问控制则保证了用户的访问都是在可控的环境下进行的。同时，数据到达用户终端时，也能够将其限制在安全域中。

目前越来越多的国际企业都开始坚定地向 SaaS 交付模式转变。Vmware 这一方案也是如此，交付模式为 SaaS 按月订阅，可以支持按设备数量订阅，或是按用户数量订阅。虽然一定程度上这代表了未来的发展趋势，但国内的用户场景与交付环境与国外有较大区别，就数据访问安全域这个领域来说，除互联网行业外，国内的政府、金融、运营商等行业，未来几年将仍以私有化交付 + 按终端计费的模式为主。

Hysolate

作为 2018 年 RSAC 创新沙盒大赛的十强选手，以色列安全公司 Hysolate 成立于 2016 年 6 月，它通过虚拟化技术实现了终端硬件与企业工作空间的几乎完全隔离，用户的所有操作与交互对象，包括操作系统以及运行于操作系统之上的所有应用，都是以虚拟化的形式存在，每个虚拟化空间都是相互独立的。某种意义上实现了“软件定义终端”，以此实现了数据访问在终端侧的安全管控。

乍一看起来，Hysolate 的方案与 VDI 很像，最大的不同之处在于 VDI 的应用与数据都是在服务端，然后以远程桌面的形式在用户侧呈现。Hysolate 则只有管理侧是在云端，应用与数据都在用户侧的虚拟化隔离区域。对用户来说，就像同一个本地终端运行着两个不同的桌面系统，以此实现安全的隔离工作空间。

在 RSAC 十强之后，截至 2021 年，Hysolate 还相继参加了多个类似的安全赛事与评选，都有取得不错的成绩。侧面说明，在国际安全市场上以 Hysolate 为代表的数据访问安全域（Hysolate 自己定义为“隔离工作空间”）始终受到业内的持续关注。

一知安全

在国内，成立于 2018 年的一知安全作为该领域的代表企业，实现了数据访问在终端侧与网络通道的安全管控。

不同于 Hysolate 的完全虚拟化，一知安全使用的是“半虚拟化”技术隔离数据工作空间，使安全域、非安全域独立安全工作。如此一来，即保留了非安全域中用户自由使用的灵活度，同时也复用了物理机的硬件性能，避免了 VDI 模式下的性能瓶颈影响安全域中的工作。数世咨询了解到，一知安全已经将这一技术在 Windows，MAC 和信创等多个终端做了适配。

在网络侧，一知安全采用的是本报告前述核心能力与技术要点中提到的基于零信任理念的 SPA 网络隐身单包授权认证、无虚拟网卡隐身网关等技术手段，收敛攻击暴露面的同时，还避免了流量嗅探等带来的风险，解决了数据访问在网络侧的安全隐患。

一知安全核心团队来自于国家某监管机构，具备实战技术背景，相比一般

的安全初创企业，其技术底蕴会更为扎实。因此，其产品技术方案也带有明显的 APT 防护痕迹。例如，在终端侧针对 DLL、账号等高级别攻击异常行为做了重点识别，同时通过攻击链可视化等手段，突出显示攻击者行为。除了来自于外部的攻击，对于内部人员的越权与违规行为，会基于详细的业务访问数据，针对性的做出细粒度的访问管控，甚至提供了终端用户操作行为的 UEBA。通过“技术 + 管理”的思路，帮助用户建立访问控制机制，实现“数据不落地，落地不泄密”。

数据访问安全域的价值

最后，总结下数据访问安全域的主要价值：

1. 数据流动的安全保障

通过数据访问安全域这一技术实现方式，企业与外包机构之间、企业内部各分支机构之间、企业数据中心与员工终端之间等场景下，敏感数据的流动过程始终在零信任理念下的各安全域间流转，有效保护商业秘密和敏感数据在流转环节被潜在攻击者窃取，避免经济损失。

2. 数据访问的安全隔离

“安全域”能够使得各类终端环境对数据的使用始终在“域”进行，对数据的传输和访问始终处于零信任框架中，减少业务和数据的暴露面，无论是访问过程还是事后审计，都能够达到安全可控的要求。例如，在外包场景中，核心敏感数据始终保持在“安全域”中，对外包机构来说，数据是“不落地”的，即便外包终端突然离线，亦可以通过策略控制的方式，自动清除域中的数据。

3. 数据管理的全面覆盖

通过数据访问安全域，可以实现机构、团队数据保护全覆盖，做到统一、整体的数据保护落地，实现数据保护水桶无短板，改变以往 DLP 只能覆盖某些核心部门、业务，终端 EDR、桌管等只做策略控制，不做数据管理的问题。

4. 数据治理的降本增效，降低成本与运维复杂度

如前所述，综合采用 DLP、终端 / 桌管等产品时，在成本与运维复杂度上，

投入产出比并不理想，因此，Hysolate或一知安全这样的数据访问安全域方案，对数据的使用过程可以做到“软件定义数据生命周期”，能够为用户带来显著的降本增效。

5. 数据风险的分级管理

通过数据访问安全域，可以限制不安全的数据访问流程（如接入、访问互联网网站，打开安全性未知的文档，测试、使用第三方安全性未知的应用软件等）对终端设备可能造成的安全性风险，实现数据分级治理的目的，提高终端系统的安全性。

综上所述，数世咨询认为，数据访问安全域基于零信任理念，依托用户现有的终端基础设施，基本不影响终端侧用户原有的业务流程与使用习惯，能够为用户提供一个性价比较高且部署改造成本较低的备选方案，在技术层面与商业层面都具有较高的价值。数世咨询会持续关注这一领域。

数世咨询
Digital World Consulting

第三方中立

- 完全第三方背景
- 独立分析师团队

调研对象

- 700+网络安全企业
- 年均500+深度沟通
- 年均2000+小时访谈时长

服务对象

- 国家、行业监管机构
- 行业客户及用户
- 网络安全产品&服务供应商

服务内容

- 国家、行业智库
- 细分领域等调查研究报告
- 为服务对象提供面对面咨询
- 为产业各方提供资源对接

合作方式

- 各类报告定制
- 年度企业观察列表
- 活动赞助
- 投资FA

北京数字世界咨询有限公司（以下简称数世咨询）是国内数字产业第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布过《中国网络安全大事记》、《中国数字安全能力图谱》、《中国网络安全能力100强》、《中国网络安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，并与400余家具备原厂能力的安全企业和100余家安全行业领先者企业，以及110余家有网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动，投融资对接，安全产品与企业推荐，企业资源整合等。

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区鲜鱼口街90-2号网安小酒馆
官方网站：https://dwcon.cn
联系邮箱：dw@dwcon.cn

数世咨询
Digital World Consulting

数字安全领域中立第三方调研机构