开放数据中心委员会
Open Data Center Committee

[编号 ODCC-2022-08003]

新型数据中心高安全

技术体系白皮书



开放数据中心标准推进委员会

2022-09 发布

版权声明

ODCC（开放数据中心委员会）发布的各项成果，受《著作权法》保护，编制单位共同享有著作权。

转载、摘编或利用其它方式使用 ODCC 成果中的文字或者观点的，应注明来源：“开放数据中心委员会 ODCC”。

对于未经著作权人书面同意而实施的剽窃、复制、修改、销售、改编、汇编和翻译出版等侵权行为，ODCC 及有关单位将追究其法律责任，感谢各单位的配合与支持。

www.ODCC.org.cn

编制说明

本报告由 ODCC 安全特设组牵头撰写，在撰写过程中得到了多家单位的大力支持，在此特别感谢以下参编单位和参编人员：

参编单位（排名不分先后）：

中国移动通信集团有限公司、中国信息通信研究院（云大所数据中心团队）、中国电信股份有限公司研究院、华为技术有限公司、新华三信息安全技术有限公司、杭州迪普科技股份有限公司

参编人员（排名不分先后）：

杨海俊、邹珂龙、杜海涛、程宇、尹伟、韩敏玲、谢丽娜、江畅、王素彬、王雪荣、严菲、初利宝、王健、孙健

项目经理：邹珂龙 zoukelong@chinamobile.com

www.ODCC.org.cn

前 言

随着 5G、工业互联网、云计算、人工智能等业务的蓬勃发展，传统数据中心正在向着以“高技术、高算力、高能效、高安全”为特征的新型数据中心发展。新型数据中心作为关键信息基础设施，是网络强国、数字中国、智慧社会建设的重要基础，也是支撑我国数字经济发展的底座。

本白皮书以数据中心行业发展政策为指导，立足当前建设新型数据中心面临的安全威胁和攻击变化，创新性提出新型数据中心高安全的四大目标特征及四层三面的技术体系。本白皮书探讨了基础设施、算网一体、应用及数据等方面的安全技术要求，从系统建设、核心业务和安全运营三个维度对新型数据中心安全管理新内涵进行了系统性的总结，梳理了新型数据中心安全产品和技术图谱，最后提出了新型数据中心安全等级评估的必要性和工作方向。

由于水平有限，白皮书必然存在不足或错误之处，欢迎业界各位批评指正，大家共同开展相关领域的探讨。

本白皮书的版权归 ODCC 所有，未经授权，任何单位或个人不得复制或拷贝本白皮书之部分或全部内容。

www.ODCC.org.cn

目 录

版权声明..... I
编制说明..... II
前 言..... III
一、 新型数据中心安全发展的必要性及目标..... 1
1.1 背景..... 1
1.2 新型数据中心面临的安全威胁和挑战..... 1
1.3 新型数据中心高安全总体目标..... 2
二、 新型数据中心高安全技术体系..... 3
2.1 基础设施安全层..... 4
2.1.1 物理环境安全..... 5
2.1.2 设备自身安全..... 5
2.2 算网一体安全层..... 5
2.2.1 网络安全..... 5
2.2.2 算力安全..... 7
2.3 应用安全层..... 9
2.3.1 WEB 应用安全..... 9
2.3.2 API 应用安全..... 10
2.4 数据安全层..... 10
2.4.1 数据采集安全..... 11
2.4.2 数据处理安全..... 12
2.4.3 数据存储安全..... 12
2.4.4 数据服务安全..... 13

www.ODCC.org.cn

2.5 系统建设管理平面 14
2.6 核心业务管理平面 15
2.7 安全运营管理平面 16
三、 新型数据中心安全等级评估 18
3.1 安全等级评估的必要性和意义 18
3.2 安全等级评估思路 19
四、 展望 21

www.ODCC.org.cn

一、新型数据中心安全发展的必要性及目标

1.1 背景

作为信息社会的数字底座,数据中心已经成为推动社会发展的战略性基础设施，是助推数字经济发展的重要力量。早在 2017 年，我国就提出“要构建以数据为关键要素的数字经济，要切实保障国家数据安全，要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”数据中心作为数字经济及其数据安全的主战场，其安全问题近年来愈发得到相关政府部门、运营商和企业的高度重视。2021 年 7 月，工信部印发《新型数据中心发展三年行动计划（2021-2023 年）》，指出新型数据中心具有高技术、高算力、高能效、高安全的特征。新型数据中心在构建高效算力服务的同时，“高安全”作为其建设和发展的基本特征和要求也被正式提出。2021 年 12 月，国务院印发“十四五”数字经济发展规划通知，其中明确强调要着力强化数字经济安全体系，要求增强网络安全防护能力，提升数据安全保障水平，切实有效防范各类风险。

1.2 新型数据中心面临的安全威胁和挑战

相比于传统数据中心，新型数据中心在业务云化与数字化转型的浪潮中，主要面临三大安全威胁和挑战：

- **安全威胁面在不断增加和扩大**。随着数据中心 IT 架构不断变革，多云、混合云部署成为常态，算力设施资源从传统物理设备向虚拟化、容器化演进，各类网络及业务访问更加多元化；数网协同、数云协同、云边协同带来更多开放性，传统安全边界在逐步消失。
- **网络攻击手段和技术不断升级**。地缘政治摩擦、全球贸易争端以及日渐激烈的市场环境，攻击手段和技术越来专业化和“国家化”，迫切需要数据中心建设发展成为可信、安全、合规的运营基石，以应对当下如供应链攻击、勒索病毒等日益增多的新威胁事件以及未来的不确定性挑战。

- **安全防护产品和技术能力参差不齐**。近年来安全技术和产品迭代迅速，市场上各类安全产品日益增多，但这些产品彼此孤立、松散组合，使得新型数据中心的安全建设愈加复杂，并带来了诸多安全隐患，比如操作复杂性、可视化孤岛、安全响应复杂性、防御盲点等。

面对当下日益严峻的网络安全形势，缺乏顶层设计、查缺补漏的安全架构已经不能满足新型数据中心的安全建设需求，亟需建立一体化数据中心安全技术体系，全方位赋能新型数据中心建设发展，实现新型数据中心可视可防可控的立体化安全。

1.3 新型数据中心高安全总体目标

随着新的安全形势发展和网络安全相关法规条例的实施，新型数据中心迎来新的安全理念和技术要求。为了实现快速及时的算力安全服务、网络安全防御、数据安全存储和运营安全处置，新型数据中心高安全技术体系必须落实不同维度、不同侧重的各类监管合规要求，覆盖日常运营、安全评估、应急和重保等各类运营场景，有效识别和抵御业务访问、运维管理、开发测试、数据服务等数据中心各环节面临的外部威胁和内部风险。为此，新型数据中心的安全技术体系应达到以下四个目标：

- **安全内生**

随着开源代码等的广泛应用和数据中心内各类系统的日益复杂，数据中心内各类设备自身漏洞常常成为遭受攻击的突破点和重灾区。尤其是 IT 硬件设备和软件系统，自身的安全问题层出不穷，提升数据中心各类基础设施自身的安全性不可或缺且迫在眉睫。通过不断加强设备自身健壮性和“内置式”主动防御能力，构建主动免疫的安全体系新防线。

- **安全可视**

有力的安全防御手段依赖于对业务正常行为和异常事件的准确识别和展示，及时发现调查取证并最终确认安全威胁，才能在确保数据中心业务不受影响的情况下做到“不漏检、不误杀”。业务正常行为的准确识别，前提是必须要对数据中心资产、网络拓扑及各类生产数据实现识别认知能力，做到资产、网络、数据的可视；而只有具有对数据中心安全信息统一全局的监测视野，才能做到“一点及时发现，全网协同防御”的可视化目标。

- **融合联动**

当下新型网络攻击经常混合使用多种手段和战术，逐步渗透并侵入数据中心核心资产，这使得传统的静态的攻击威胁识别难以形成有效的防御。因此需要基于人工智能等新技术，站在数据中心全局安全的角度对主机端点事件、网络威胁事件、历史日志信息等多点异常融合分析，并实现针对安全事件的边界节点就近实时联动处置，把安全威胁扼杀在最小影响范围内。

- **绿色高效**

绿色低碳是新型数据中心的显著特征。近年来随着数据中心安全新技术的涌现，数据中心内部各类安全产品逐年增多，重复臃肿的安全产品引入和建设不仅违背了新型数据中心绿色发展理念，而且加大了数据中心运维管理复杂度，同时也显著增加了内外部业务时延。在算力时代全国数据中心集群统一高效调度的大背景下，新型数据中心的安全建设必将向着去冗余、重编配的绿色高效方向发展。

二、新型数据中心高安全技术体系

为应对内外部日益加剧的安全风险和挑战，强化以数据为核心要素的数据中心安全建设，实现安全内生、安全可视、融合联动、绿色高效的总体目标，新型数据中心需要形成“四层三面”的高安全技术体系架构。



图 1 新型数据中心“四层三面”安全技术体系架构

“四层”主建，从安全能力建设的视角，自下而上覆盖数据中心内安全防御的主要对象，分为基础设施安全层、算网一体安全层、应用安全层和数据安全层。

“三面”主管，从安全防范管理的视角，把四层安全能力协同贯穿起来，形成系统化的风险抵御和运营管理能力，主要分为系统建设管理平面、核心业务管理平面和安全运营管理平面。

数据中心各类基础设施是系统管理员的领地，其安全是数据中心安全的根基；开展数据处理、存储及服务的各类核心业务是业务管理员的领地，其安全是数据中心安全的核心；而数据中心安全监测、告警和态势感知等安全运营管理是安全团队的主战场，其安全是数据中心安全的大脑。

2.1 基础设施安全层

基础设施安全是数据中心安全可靠的基础，从设计建设角度来说主要包括两方面，一方面是数据中心的物理环境安全，包括风火水电等基础资源；另一

方面是数据中心内各类设备的自身安全，通过强化自身安全健壮性，最大程度避免被攻击利用。

2.1.1 物理环境安全

物理环境安全是指确保数据中心内一切设施有一个良好的电磁兼容工作环境，并防止非法用户进入和各种偷窃、破坏活动的发生。这涉及机房选址、规划设计、机房环境、机房管理、设备与介质管理等。如：

- 选址避开自然灾害不利或危险的地区，满足国家防灾要求。
- 具备防震、防火、防水、防静电的“四防”能力，基础设施支持 7*24 小时不中断的电力保障、访问控制及监控，满足国家新型数据中心建设标准。
- 有效的区域监控、防盗报警系统，阻止非法用户的各种临近攻击。

2.1.2 设备自身安全

设备自身安全是指设备在开发及应用过程中，自身防仿冒防篡改、抗攻击的韧性能力，主要包括硬件可信、软件可信及供应链可信等。

- **硬件可信：**硬件唯一可信根，软硬件互相校验。避免使用仿冒硬件，或者软件被篡改植入恶意代码。
- **软件可信：**软件防篡改抗攻击，软件安全启动、安全运行、安全审计等防篡改能力，并能做到进程隔离、进程级异常检测和重启、逻辑/芯片级异常检测和自动复位能力等，提升系统韧性。
- **供应链可信：**从软件安全的开源和第三方、升级补丁等相关安全来源的可信，避免系统被劫持利用。

2.2 算网一体安全层

2.2.1 网络安全

新型数据中心安全从技术上离不开网络安全的保障。随着云化、虚拟化演进，网络安全从传统网络边界安全向内移到零信任、微隔离等技术代表的新的边界安全，一层层网络安全能力叠加形成防御纵深。

- **网络边界安全**

传统网络安全措施，以数据中心为防护对象，在边界上部署如防火墙、IPS、抗 DDoS 等网络安全防护设备。对于新型数据中心来说，边界防护仍然是基本的安全保障，提供高性能高可靠的抵御外部攻击的边界隔离能力。但是，随着数据中心内部应用的弹性增长，需要传统网络边界安全产品能适应应用弹性部署的要求，可做到池化部署能力，向 SDN 编排、低时延等技术能力演进，实现资源编排（突破单设备性能瓶颈）、流量编排（突破设备协同瓶颈）和策略编排（突破部署效率瓶颈）。

- **内移边界安全**

IT 架构云化虚拟化后，数据中心内东西向流量持续规模增长。东西向互访连接增多使得数据中心网络边界内移到区域边界、微服务边界。当前微服务间存在合理的流量访问关系，同时也存在恶意的探测、攻击等。这使得传统网络边界信任机制被打破，内网外隔离的传统方式已经无法适应业务 IT 化转型后的安全发展需要。对于新型数据中心，在原有网络边界安全的基础上，基于零信任技术实现基于数据模型访问关系的实时应用访问行为监控成为新的要求。

- **横向流量安全**

横向移动是现代网络攻击的重要部分，它充分利用了不安全的低级网络资产及内网账户保护不力的漏洞，给新型数据中心安全带来了严重威胁，故横向流量安全能力是新型数据中心网络安全的重要补充。数据中心的业务主体是应用和数据，基于业务逻辑清晰划分防御对象，建立基于微分段的安全策略保护，避免非信任流量扩散。同时，基于业务链技术把风险流量引流到“监控/授权”

模块联动安全分析处置，实现微隔离。通过微隔离技术与零信任能力的叠加，可以把新型数据中心面临的新安全威胁风险控制在最小影响范围。

总的来说，新型数据中心网络安全需具有南北向和东西向边界防护能力、基于控制器的资源池化编排能力、基于虚机/微服务的微隔离能力及基于零信任技术的网络访问保护等特征，其安全基本结构如下：

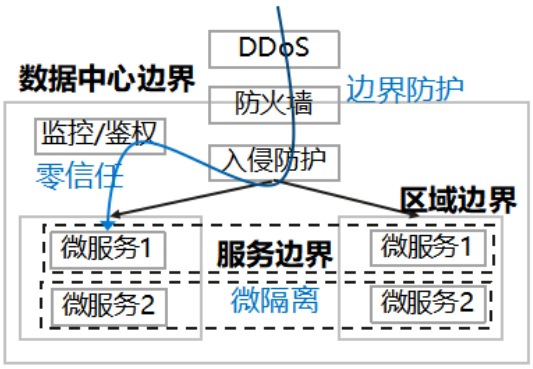


图 2 新型数据中心网络安全基本结构

2.2.2 算力安全

- **算力平台安全**

当前虚拟化和容器化技术作为提供新型数据中心算力的基础平台，突破了传统操作系统与物理硬件之间的界限，在算力资源集中化管理、提高硬件利用率、异构算力资源整合等方面发挥了关键作用。但底层硬件资源的共享也带来了一定的安全风险。为此，需要进一步做到虚拟层隔离安全和虚拟交换安全。

虚拟层隔离安全：同一物理机上不同虚拟机之间应做到资源安全隔离，避免虚拟机之间的数据窃取或恶意攻击。但当前数据中心内仍存在虚拟机跳跃、虚拟机逃逸、拒绝服务攻击和 VMBR（Virtual Machine Based Rootkit）攻击等安全隐患，故针对虚拟层开展定期配置检查和及时漏洞补丁更新，确保 vCPU 调度隔离、内存隔离、磁盘 I/O 隔离安全，化解虚拟层隔离安全风险十分必要。

虚拟交换安全：OVS 等虚拟交换机为数据中心内东西向，尤其是同宿主机算力单元之间的流量交换提供了极大便利。但其作为部署在硬件服务器内的新型软件交换设备，区别于传统物理交换机，其安全管理和策略控制极易忽视，同样存在安全风险。因此，虚拟交换机的流量可视化是虚拟交换安全的基础，在此基础上还可考虑增加额外的防护手段，如部署虚拟防火墙等。

- **算力单元安全**

主机系统作为新型数据中心算力提供的基本单元，也是绝大多数数攻击者的最终入侵目标。开展算力单元安全防护，进行常态化的威胁检测和防御，避免主机劫持事件的发生是新型数据中心整体安全的最后一道也是最有效的防线，其重要性不言而喻。具体手段包括基线核查、异常行为监控、漏洞管理及病毒防护等。

基线核查：主要针对主机配置的安全性和合理性进行检测，避免过度的暴露面带来不必要的风险。例如主机上仅开放少数几个端口用于业务与维护使用，有效应对一些高危端口或未知端口带来的病毒传播；制定严格的访问授权、密码管理等统一的主机安全策略等。

异常行为监控：支持对防暴力破解等异常登录行为、非法数字货币挖矿等算力盗用行为、域名劫持等算力劫持行为，以主机维度或用户维度建立访问和通信的大数据画像，开展异常行为监测和告警。

漏洞管理：一方面需要定期扫描主机漏洞并及时安全加固，严格测试和评估新发布补丁的兼容性、可用性、可能带来的副作用及采取的相应缓解措施。另一方面，虚拟机模板、容器镜像存在系统漏洞将进一步扩大安全风险，故需要尽量裁剪不必要的软件组件或模块，构建最小化系统；并增加如容器镜像签名等技术手段来确保系统的完整性。

病毒防护：部署防病毒软件，对各类病毒、蠕虫、恶意代码、木马等恶意文件和进程动态查杀及隔离，确保斩断病毒传播、寄生的每一个节点，实现病

毒的全面防范。当前由于勒索攻击威胁加剧，新型数据中心的病毒防护应能够识别勒索软件攻击的典型症状，一旦发现网络中 C&C 异常通信或者文件异常加密等可疑活动，应可在攻击者开始勒索之前预先发出告警。

- **算力服务安全**

随着产业数字化进程加速，未来算力需求将持续放大，算力或将成为一种可交易商品，从当前公有云数据中心算力服务的孤岛模式向全网算力如“水电”一样便捷获取的公共服务演进。由此带来的算力调度安全和算力交易安全也需要逐步纳入新型数据中心安全建设要求中。

算力调度安全：未来算力网络调度平台通过聚合海量的算力资源，将形成可持续扩张的全国一体化算力服务资源池。因此需要建立一个安全可信的调度机制，实现算力资源的安全流通，才能满足国家重大战略和医疗、交通、安防、教育等各行业对算力服务的需求。

算力交易安全：当算力成为一种可交易商品后，可基于区块链、共识机制与算法、智能合约等技术构建可信算力交易平台，对多方泛在、多样算力进行运营计费，保证算力交易的安全可控、隐私高效。

2.3 应用安全层

2.3.1 WEB 应用安全

随着 Web 技术的普及，越来越多的应用基于 Web 平台部署，Web 应用是数据中心对外提供的主要业务。而由于 Web 应用自身多采用开源架构和开放服务的特点，其常成为应用安全攻击的入口。为实现 Web 应用安全，在新型数据中心内部署 Web 防护及网页防篡改模块，是主要的防护手段。

- **Web 防护**

通过智能引擎识别已知攻击行为，包括 SQL 注入、XSS、命令注入、文件上传、反序列化攻击等常见的 Web 攻击行为，同时加强识别未知威胁及 0day 攻击行为，保障基于 Web 的业务系统安全可靠运行。

- **网页防篡改**

应用内核态文件驱动过滤技术，阻止攻击者通过 Web 操作系统和服务程序的漏洞，获取 Web 服务器的控制权限后进行非法的 Web 操作，包括内容篡改、数据盗取或恶意代码植入等。

2.3.2 API 应用安全

随着业务的云化发展，新型数据中心内大量的云服务通过 API（如 Restful API）的形式对外提供业务和管理接口。考虑到 API 对云服务承载的重要功能和其在 HTTP 应用层面临的安全威胁，新型数据中心需要考虑把 API 视为云服务至关重要的安全边界，采用多重机制和措施进行重点保护：

一是建立动态的 API 接口管理及使用机制。通过流量学习等手段来梳理活跃的 API 应用和暴露的 API 接口，依据 API 的状态变化并结合用途属性进行分级分类,区分在用 API、废弃 API、测试 API、异常 API 和未知 API，形成动态更新的 API 接口清单，及时发现 API 应用隐患。

二是采用专用的 API 应用网关设备。一方面增强 API 调用的认证和权限控制，限制 API 调用速率；另一方面通过部署 API 检测和攻击防护技术，识别 API 访问接口所遭受的各种自动化脚本、爬虫工具和 BOT 工具的扫描和恶意调用，从而提升应用安全的整体防护能力，避免 API 滥用、盗用行为的发生。

2.4 数据安全层

数字经济时代，数据安全是新型数据中心安全建设的核心。新型数据中心数据安全应借助组织人员的安全能力和管理制度，在数据安全分级分类、安全

可视的总原则下，以“数据采集安全”为基础、“数据处理安全”为关键、“数据存储安全”为保障、“数据服务安全”为目标，构建全生命周期的数据安全流程，实现数据的完整性、保密性、可用性和持久性。

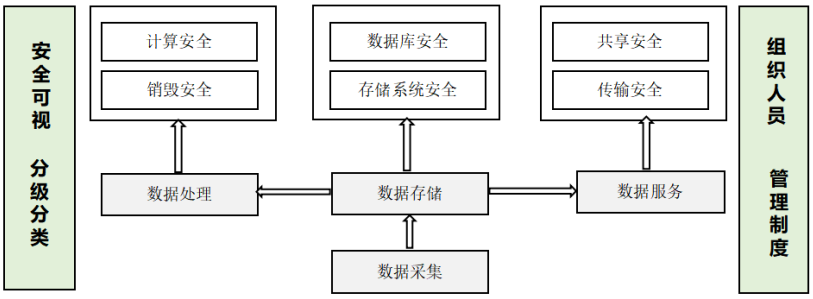


图 3 新型数据中心数据安全治理结构

2.4.1 数据采集安全

数据采集的目的是获得有价值的数据资产，采集应严格按照《网络安全法》、《个人信息保护法》等相关法律法规和行业规范执行，数据中心内数据采集的方式主要包括应用数据通过网络采集、数据中心内系统日志数据采集等。组织开展数据采集活动的过程中，应确保数据采集的合法性、正当性和必要性：定义采集数据的目的和用途，明确数据来源、采集方式、采集范围等内容，并制定标准的采集模板、数据采集方法、策略和规范；对于初次采集的数据，需采用人工与技术相结合的方式进行数据采集确认；最小化采集数据，不收集与提供服务无关的个人信息和重要数据；对数据采集环境、设施和技术采取必要的安全管理措施。

对采集的数据进行分类分级是实现后续环节数据安全的前提。新型数据中心应对采集数据的存储位置、存储格式、存储内容和大小，依据国家《数据安全法》、《个人信息保护法》等法规及《基础电信企业数据分类分级方法》等行业相关标准制定数据分类分级体系。基于数据安全监测及数据防泄漏设备，针对不同数据级别设置安全保护策略，为后续数据处理、数据存储和数据服务提供依据。

目前业界对数据的分级分类缺乏有效实施经验，主要还依赖人工处理，工作量大且效率低，而基于关键字、知识库进行自动分类分级误判率高。新型数据中心面对各行各业数据，数据的安全分级分类应借助机器学习构建的知识算法，将专家经验和方法固化为规则模型和识别引擎，通过自动化、智能化的分类分级技术手段，提升数据分类分级的质效。

2.4.2 数据处理安全

新型数据中心的数据处理安全主要解决数据的隐私权问题，包括数据隐私计算和数据的删除销毁。

- **数据隐私计算**

由于数据处理需要涉及多源、泛在的算力节点，无法保证每个算力节点都是安全可靠的，数据分配到算力节点进行计算的模式会使数据面临隐私泄露的风险，因此需要借助包含安全多方计算、可信执行环境、联邦学习等隐私计算技术来实现数据的“可用不可见”。

- **数据的删除销毁**

依据数据中心合规政策和业务发展需求，对敏感数据或老化过时数据进行删除销毁，也是数据处理安全有效的重要环节。建立数据删除销毁策略和管理制度，明确数据销毁的场景、销毁对象、销毁方式和销毁要求，通过覆写法、删除、格式化等清零操作销毁内存和硬盘中的数据，通过物理摧毁、消磁等方式实现各类数据存储介质的有效销毁，杜绝信息泄漏风险。建立数据销毁的管理机制，对数据删除销毁操作保存完整记录，满足行业标准和安全回溯要求。

2.4.3 数据存储安全

新型数据中心的数据存储安全是指数据存储过程中的机密性和可靠性，主要涉及底层的存储系统和数据库中间件。

- **存储系统安全**

对于不同存储系统，例如磁盘阵列、分布式存储、全闪存存储等，其存储的机密性一方面通过存储系统自身的数据分块/卷及散列来保证，另一方面也可采用基于密钥的数据加解密技术，通过专用硬件设备实现敏感数据加密存储。而为了实现数据存储的高可靠性，存储系统应通过存储前的一致性检查、数据分片冗余、自动快照、多副本备份与恢复等技术手段，为不同级别数据设置不同数据可靠性策略，确保数据的完整性、一致性、准确性和持久性。

- **数据库安全**

数据库作为承载关键生产经营数据的主要载体，需要建立完整的数据库安全防护能力，涵盖数据库上线、使用、运维、迁移全过程：数据库上线前通过安全基线进行自动化的安全配置检查，确保数据库不带安全隐患；使用过程中，通过对数据库访问和操作行为进行全面精确的审计和智能预警，防止核心数据的泄露与破坏，确保数据库访问关系、数据库攻击威胁清晰可视；在运维和迁移过程中，采取针对性的技术和管理措施，建立标准化的操作流程，确保数据库运维和迁移安全。

2.4.4 数据服务安全

站在数据流通的角度，新型数据中心业务的本质就是通过数据传输和共享向用户提供数据的服务。在技术方面，数据传输和共享应该通过统一的身份管理、权限管理和认证管理确保数据服务对象的合法性；通过 VPN、应用层 TLS 与证书管理等通道加密技术确保数据的传输安全，防止数据监听、窃取、伪造和重放等数据传输风险，从而保证数据服务的安全性。同时，数据的传输和共享还应防止敏感数据泄漏，通过在数据传输边界部署敏感数据识别设备，通过语义识别、机器建模与匹配等技术实现对敏感数据的监测和告警。

对于因业务开展需要涉及出境服务的数据，应按照《数据出境安全评估办法》进行数据出境的风险自评估、申报和监测，保护国家信息安全。

2.5 系统建设管理平面

系统建设管理是新型数据中心的安全根基，通过将安全建设理念植入到数据中心系统建设的规划、设计、集成、评估、交付全流程，消减数据中心的薄弱点，才能筑牢抵御日常威胁的基层防护篱笆。

一是加强顶层设计。统筹系统建设的安全目标，自上而下逐层开展安全架构设计，同时做好系统扩展和迭代的长远考虑，用系统化的理念构筑韧性的安全架构。对于系统集成，应保障安全建设在整个系统建设中的投资占比，并对安全设备和技术方案进行统一规划，避免安全设备五花八门、各自为战，冗余重叠。

二是遵循隔离原则。数据中心系统规划、设计、集成和评估均应充分考虑安全域隔离设置原则，缩小攻击事件的影响范围。通过模块化设计，物理上划分接入 DMZ 域、核心生产域、管理维护域，加强区域边界安全。新型数据中心还应划分独立的测试验证域，一方面对新安全设备部署、安全策略调整、补丁升级等进行严格的离线仿真测试；另一方面用于生产系统安全应急演练和人员安全技术培训。

三是充分安全评估。在系统集成完成交付前，应进行充分的安全评估。通过对安全资产的主动探测识别，梳理各类 IT 软硬件资产和数据资产的风险，评估潜在的供应链安全；评估安全威胁的潜在传播途径，保证最有效的防护措施应用到可能被攻击的关键线路上；评估安全区域的隔离效果及安全事件发生的应急预案，杜绝安全事件触发系统瘫痪等重大隐患。

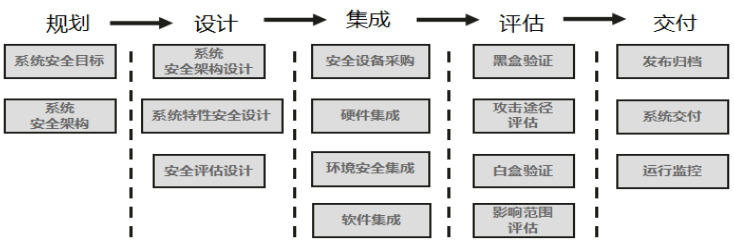


图 4 新型数据中心系统建设管理流程安全框架

2.6 核心业务管理平面

业务的安全管理是新型数据中心安全的核心。具体来说需要分为业务安全设计和业务生命周期安全管理两部分考虑。

- **业务安全设计**

在业务规划设计时，需要从业务和威胁两个视角来分解安全设计目标。如下图所示，从业务视角不仅要遵从网络安全法等国家相关标准，还应考虑运营商、政务、金融、医疗、视频、电商等不同行业的业务特点，将具体行业业务作为安全设计的输入，合理制定安全目标；再通过业务流识别关键价值资产，建立风险假设。而从威胁视角出发，应从业务信息流分解目标网规划，通过数据流分析风险暴露面和攻击路径，形成脆弱性评估结论，用于指导核心业务安全解决方案建设和管理。

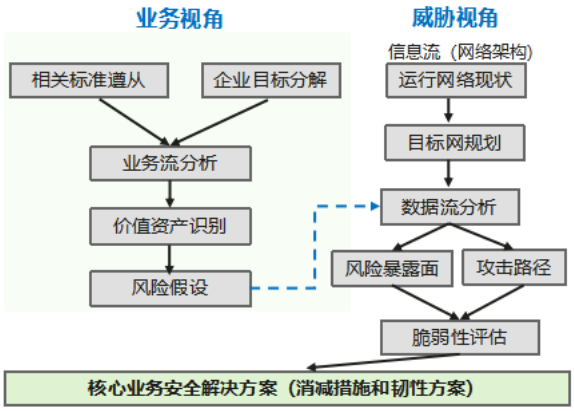


图 5 新型数据中心核心业务安全设计

- **业务生命周期安全管理**

随着以微服务、DevOps、持续交付为显著特征的云原生应用的发展，新型数据中心业务的安全管理要求从原来以运行时防护为重心进一步前置，需要安全赋能到业务的需求、设计、开发、测试、交付等生命周期的各个环节。

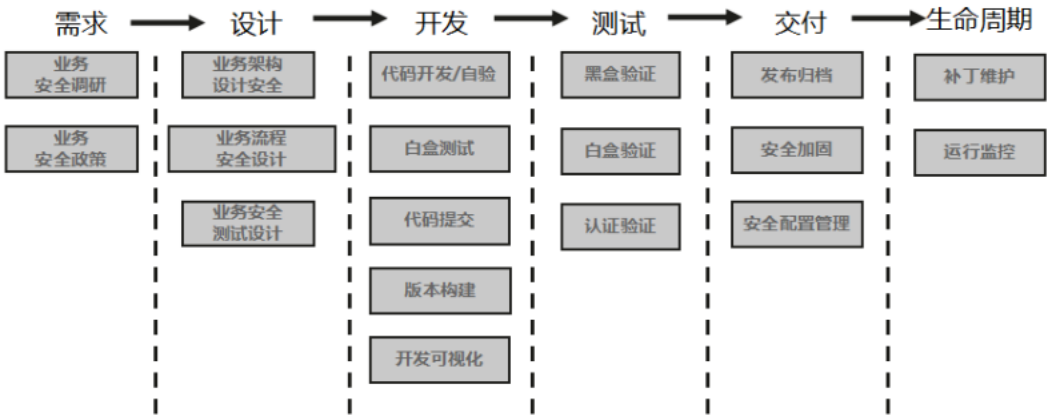


图 6 新型数据中心业务生命周期安全管理

如上图所示。在**需求阶段**，需要对业务开发模式及安全现状进行充分调研，评估最新安全监管政策和业务场景的安全特性，明确业务的安全需求。在**设计阶段**，需要进行进一步的风险分析，从业务框架、业务流程和测试验证维度进行详细业务安全设计。在**开发阶段**，需要业务开发者将增强抵抗力的安全理念应用于代码开发阶段，通过部署开发安全工具，将各种安全能力与 DevOps 流程结合，高效准确地识别业务开发中的安全缺陷及漏洞，实现安全防护“左移”。在**测试阶段**，需要制定严格的黑白盒测试方案，尝试发掘业务否存在交易数据篡改、接口未授权访问、关键数据明文传输等安全设计缺陷。在**交付应用阶段**，应结合业务开放的端口和属性，对所在的硬件服务器、操作系统、数据库及应用中间件等，通过补丁升级、强化帐号安全、优化访问策略等方式进行安全加固和安全配置，提升业务安全防范水平。

2.7 安全运营管理平面

安全运营管理是新型数据中心感知安全威胁与响应处置事件的大脑，在新型数据中心安全中起决定性作用。安全运营管理相关技术也是近年安全领域最活跃的技术，诸如态势感知、UEBA、威胁情报、XDR、SOAR、安全知识图谱、蜜罐等技术层出不穷。新型数据中心需要建设统一的安全运营中心，提高安全事

件的前瞻性预测能力，开展常态化安全监测、威胁情报分析，对安全事件实现自动响应及快速处置，保障新型数据中心的运营安全。

在运营管理制度上，新型数据中心一方面应以安全合规为驱动，主动落实国家及行业相关安全政策法规，响应安全等级评估及等保评测；另一方面应以业务目标为驱动，匹配业务的安全属性，制定针对性的安全运营管理策略。

在安全运营技术上，新型数据中心应以安全事件为驱动，围绕安全运营中心，构建监控检测、威胁情报、响应处置、能力沉淀的有机衔接和闭环体系，支撑平战一体的安全态势研判及应急指挥。而安全运营中心应以泛在感知、智能分析、主动防御、自主学习为目标向着安全运营大脑持续演进。

- **监控检测：**通过规模部署全流量安全监测探针等，实现对各类风险流量、可疑报文和安全漏洞的 7x24 不间断监测，并及时上报。
- **威胁情报：**基于外部情报设立动态的威胁情报数据库，并利用人工智能与大数据技术建立威胁模型，对监测到的可疑行为和漏洞开展自动化、智能化的安全运营分析和预警。
- **响应处置：**将发现的安全威胁结合安全数据分类分级进行归一化关联处理，实现各类告警的分级分类上报及安全态势可视，并联动各层级安全防护能力协同防御。
- **能力沉淀：**打造专业的数据中心安全运营团队，分层分级、专职专责，做好基于事件响应追踪、威胁情报和处置措施的分析学习，依托智能化安全运营工具实现安全策略的动态更新和编排，从被动防御向主动威胁狩猎进发。

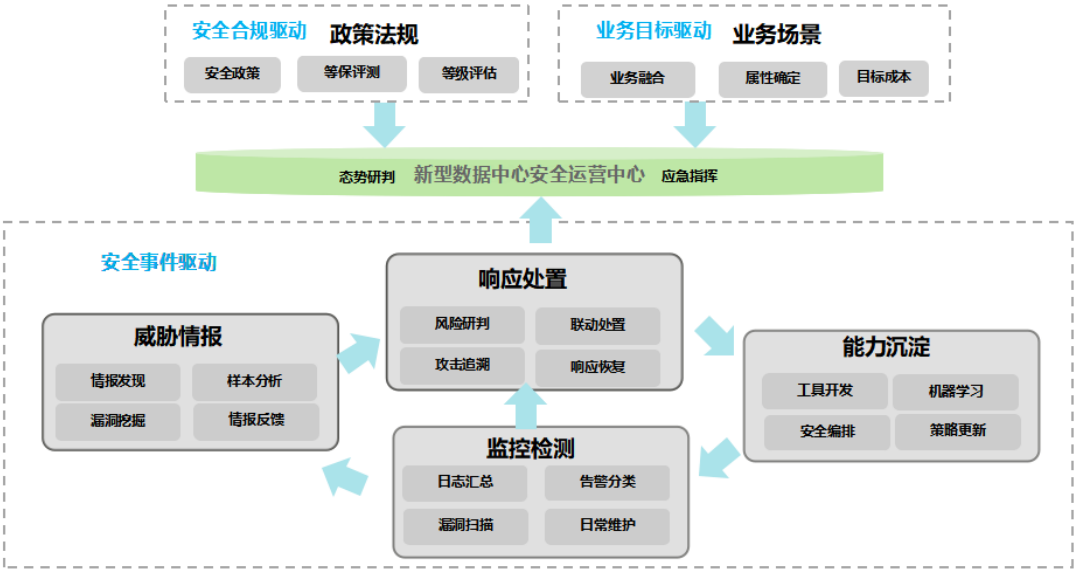


图 7 新型数据中心安全运营管理技术框架

三、新型数据中心安全等级评估

3.1 安全等级评估的必要性和意义

国家政策和重大网络安全事件是数据中心的安全建设的主要驱动因素。随着国内外安全形势的变化，新型数据中心的高安全标准将要求我们更加注重实战效力，注重安全与系统建设同步、与业务场景深度融合的“一体化”安全发展。

我国数据中心安全技术迭代迅速，围绕“四层三面”的安全技术体系，所涉及的数据中心安全产品和技术繁多，如图 8。但当前大多数的数据中心安全建设缺乏统一规划和标准，各数据中心建设者、运营商部署的安全技术能力之间差异较大、应用不一，这种相对粗放的建设模式不但导致了数据中心安全产品“烟囱式”孤岛发展，而且也极易带来整体安全技术防御体系的疏漏。

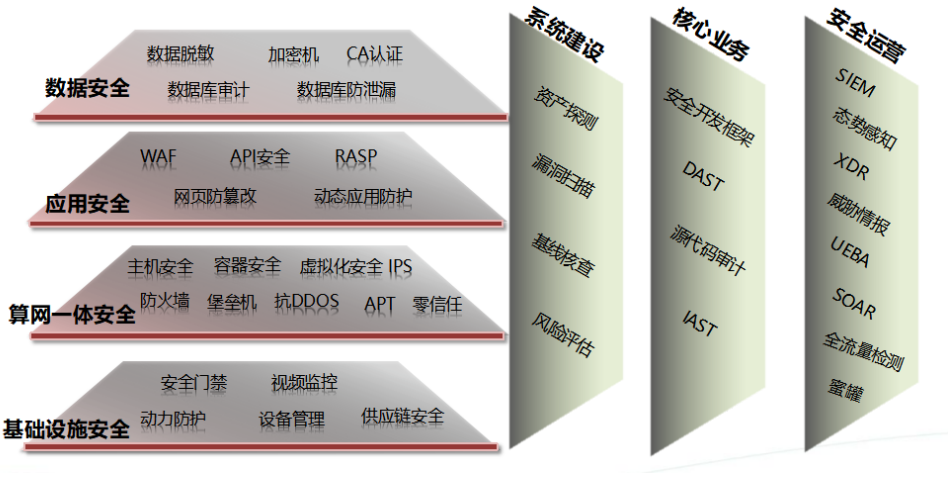


图 8 数据中心现有安全产品图谱

同时，在具体安全产品和技术能力的评测方面，目前业界普遍采用的还是基于商用测试仪表或知名第三方工具的静态测试方法，大多数只能针对已知攻击报文或威胁特征的防御效果进行简单的验证和识别。传统的安全测试方法与真实的安全攻击手法、事件场景差距较大，过于依赖特征辨识，缺乏动态交互式的多阶段攻击模拟，很难满足后续新型数据中心的安全产品和技术能力评测工作需要。

因此，推动建立我国新型数据中心的安全等级评估标准和机制，为数据中心的安全建设和技术能力提供指导标准和评估、测评方法，势在必行：

一是安全等级评估将评测数据中心安全产品和技术的优劣，推动数据中心安全技术能力的整合优化及联动协同，切实提高数据中心的安全建设水平和效率。

二是安全等级评估将进一步引导、健全我国数据中心的安全能力和技术发展，总结数据中心安全治理优秀经验，提升数据中心安全事件应急处置水平与防护韧性。

3.2 安全等级评估思路

基于新型数据中心高安全技术体系架构，围绕安全防范管理三大平面“系统建设”、“核心业务”、“安全运营”，根据新型数据中心的安全水平成熟度，可划分为四个等级：L1（静态）、L2（动态）、L3（自动）、L4（意图），见图 9。

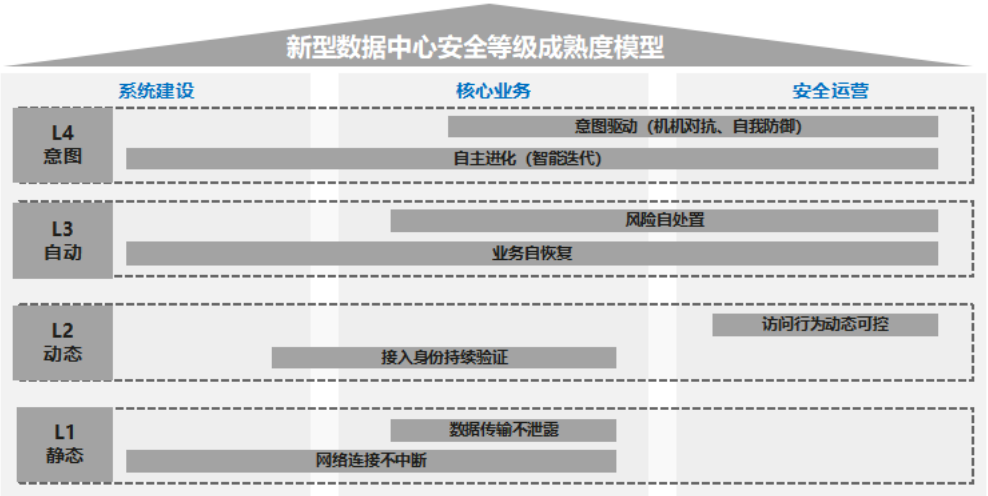


图 9 新型数据中心安全等级成熟度模型

- **L1（静态）**：通过离散的，一次性的技术手段，实现网络连接不中断，数据传输不泄露，确保网络实现最基本的可达能力和数据保护能力。
- **L2（动态）**：通过持续的，随业务环境改变的身份认证，环境感知，行为分析，实现接入身份安全，访问行为可控，应对身份和行为的不确定风险。
- **L3（自动）**：面对恶意和非恶意的行为或攻击，网络可以自动感知、自动分析、自动溯源并联动处置，实现风险自处置、业务自恢复，应对异常情况下业务保障的不确定性风险。
- **L4（意图）**：基于业务意图，网络通过对已知/未知风险进行自主学习，持续进化，并进行智能分析和决策，选择并部署最佳防护方案，最大程度消除潜在风险，实现自主防御，自主进化的确定性新型数据中心网络。

新型数据中心安全技术体系中的系统建设、核心业务及安全运营三平面贯穿了全部安全技术能力，这不仅为新型数据中心高安全能力提供了管理视角，同时安全等级评估的推进也可基于此三方面开展：

- 系统建设管理安全评估：深入探究数据中心系统建设的安全设计，从顶层规划设计的思路、安全域划分的逻辑、安全产品部署的层级和联动、系统交付前的安全评估结果等多维度考察安全建设的合理性、前瞻性。针对各层级安全产品，开展安全技术能力测评，评估防护效果和性能。
- 核心业务安全能力评估：评估数据中心核心业务需求设计、开发测试、交付运行全流程的引入的安全管理制度和技术手段，验证业务安全开展的合规性、制度的完善性及有效性。
- 安全运营能力：通过定期组织开展基于 ATT&CK 等动态模型的安全攻击模拟和事件演练，检测数据中心整体防御能力和安全运营效果，确保新型数据中心安全达到可控可视的基本能力，并促进向风险感知、自主决策的高等级安全运营发展。

四、展望

当前，以算力为核心生产力的数字经济时代正加速到来。新一轮新型数据中心基础设施建设正在全国各级枢纽节点全面推进，原有“老旧小散”的传统数据中心加快改造。作为各个行业信息系统运行的物理载体，数据中心安全建设和技术发展对其实现安全可靠的行业支撑乃至信息通信产业的可持续发展至关重要。

为切实贯彻落实国家战略部署，统筹引导新型数据中心的高安全建设，推动实现安全内生、安全可视、融合联动、绿色高效的总体安全目标，助力打造新型数据中心高质量发展新格局，我们提出以下倡议：

一是共同加强数据中心的安全建设，推动数据中心相关安全技术发展，促进全国数据中心安全的标准化和能力协同。推动数据中心安全团队技术交流和知识共享，共建互信互融、合作共赢、责任共担的数据中心安全技术生态。

二是共同推进数据中心安全等级评估，联合产业上下游重点企业共同研究制定面向新型数据中心的安全等级评估标准规范，建立健全数据中心安全等级评估标准和评测体系，通过评优评级方式引导新型数据中心的高安全建设和运营。

三是共同构建专业权威、动态交互的安全测试平台及测试能力，对数据中心安全产品和技术能力进行多维度“比武”评测，为数据中心安全建设提供技术支撑。



ODCC服务号



ODCC订阅号