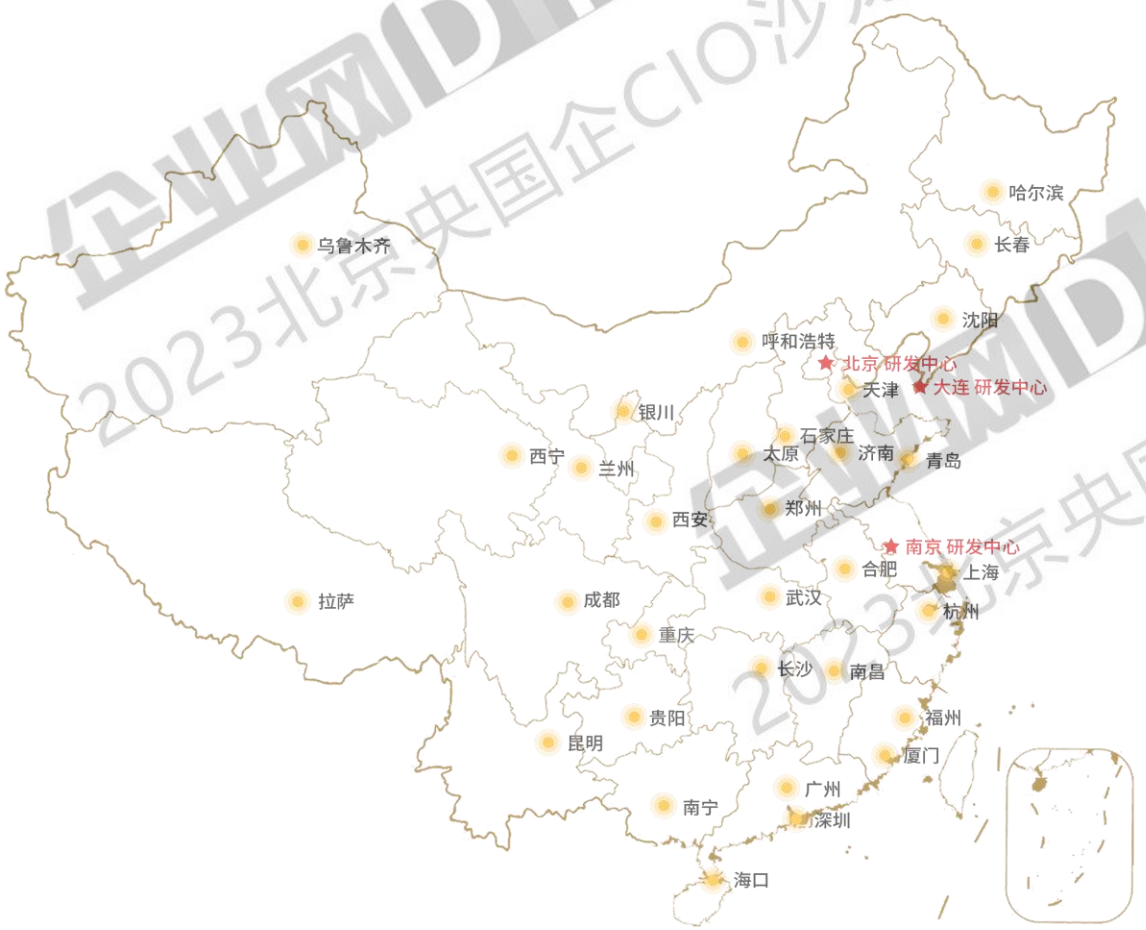
数字化安全工作空间
助力企业数字化转型

指掌易科技

2023年6月3日

公司简介：专注于移动业务安全领域，行业领先



公司：成立于2013年11月，总部位于北京，广州、深圳、珠海、上海、成都、武汉、厦门、西安等地设有分支及服务机构，在北京、南京、大连设有研发中心。

业务：专注于**移动业务安全领域**，基于自有核心技术，提供业务移动化整体方案与服务,已服务政府、制造、金融、育等20多个行业超过**2000+**家客户。

团队：核心团队均拥有超过10年的移动业务与安全领域从业经历，团队兼具移动互联网与企业服务背景。

服务：全国各地销售、售前、咨询、实施、售后专家提供专业的本地化支持与服务，整合逾百家合作伙伴能力， 涵盖移动终端、移动办公应用、行业应用以及扩展安全领域，为客户提供整体解决方案。

业务模式：数字化工作空间+零信任，驱动企业数字化转型

指掌易

数字化工作空间+零信任

万物互联为数字化混合工作模式发展奠定基础

多场景数字化混合工作模式逐渐成为常态

Anytime
任意时间

Anywhere
任意地点

Any Endpoint
任意终端设备

智慧国企

金融交易

数字政务

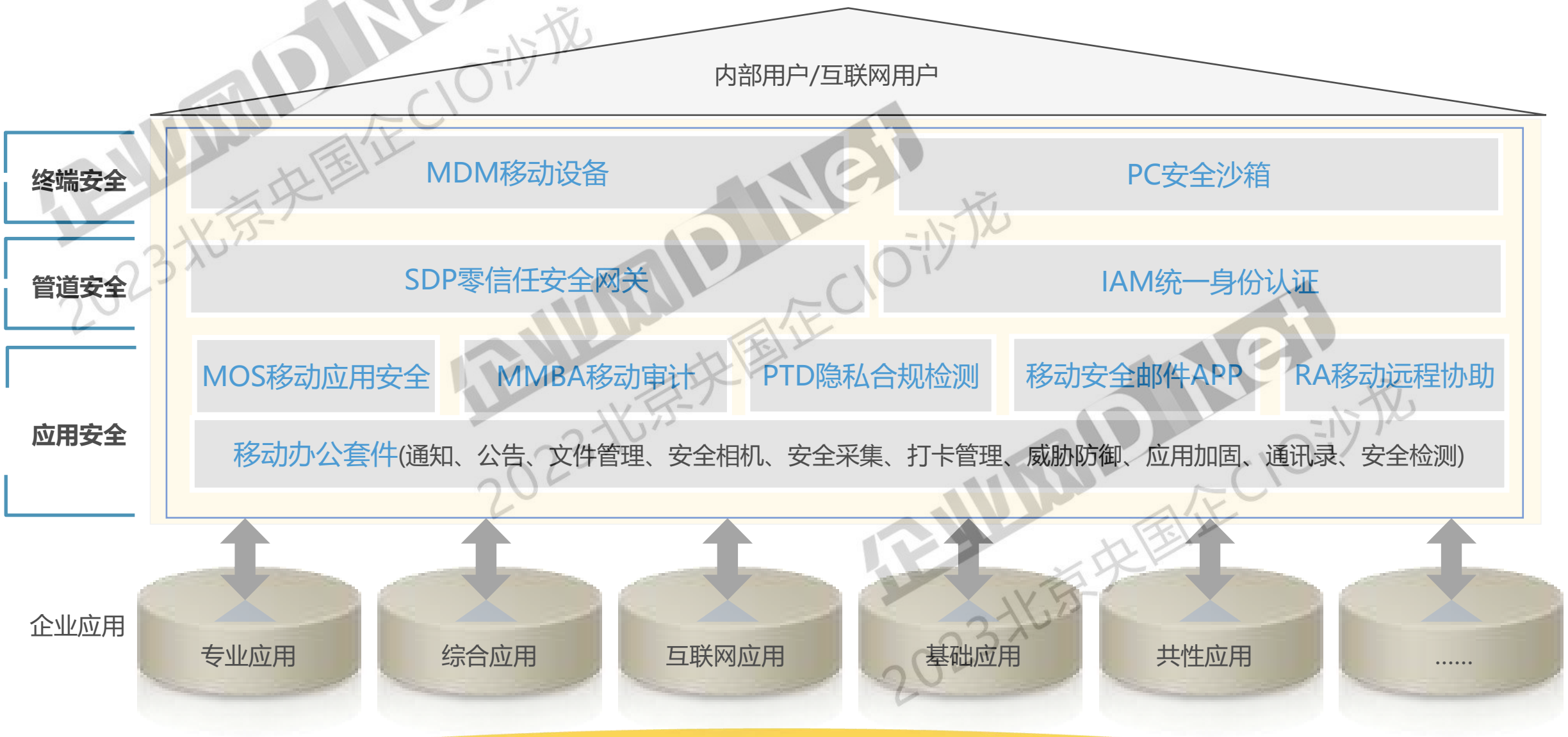
智能制造

智能交通

掌上军营

全栈产品：以端管云一体化移动框架构建全线产品

指掌易



PART
01

数字化办公安全建设任重道远

数字化办公发展三个阶段

概念：数字化工作空间在企业中典型的业务场景为“**数字化办公**”，主要以信息交互，突破传统“时空”观念，连接“人”为目的，实现信息有效分发、使用，确保“各取所需”、“数尽其用”。

物理办公

1.0 面对面

- 传统办公限于“时空”制，信息交互以实时、面对面沟通为主
- 以“点对”或会议形式进行信息传递、沟通
- 交互工具多以纸质材料为主

移动办公

2.0 可移动

- 实现“移动”办公后，信息交互方式更加灵活，打破“物理界限”，信息分发、流转效率更高
- 信息交互工具更多以移动端APP为主

数字化办公

3.0 超越时空

- 数字化办公时代，信息交互以"在线”为主，突破”时空“限制传递信息
- 信息交互可实现多人在线协助，”各取所需“更为可能
- 交互工具以平台以及垂类产品为主

指掌易

数字化办公安全产生要素

宏观环境

□ 信创环境

”国产替代“趋势明显，自主创新意识增强

□ 数据安全保护

数据隐私、在线安全已成为数字时代健康发展的基础

□ 隐私保护

提高数据安全等级，有效解决数据泄露，保障数据安全

终端设备碎片化

□ 设备

PC、手机、平板电脑

□ 操作系统

Andriod、IOS、鸿蒙

办公场景碎片化

□ 任意地点/时间

公司

家庭

娱乐场所

通勤区域

休息场所

数字化办公带来数字安全挑战

指掌易

数字化办公过程中，通常会因为终端、身份、访问、网络、数据等各方面带来安全风险和隐患。

办公业务在互联网及云上等不同环境下，其面临的病毒威胁、攻击入侵风险急剧增加，用户通过网络接入和访问，其安全风险巨大

③网络接入如何确保安全

办公业务数据的访问、存储、传输、外发，在整个数字化办公过程中，可能任一环境出现漏洞或未加防护，将直接导致数据被泄露

④业务数据如何安全流转

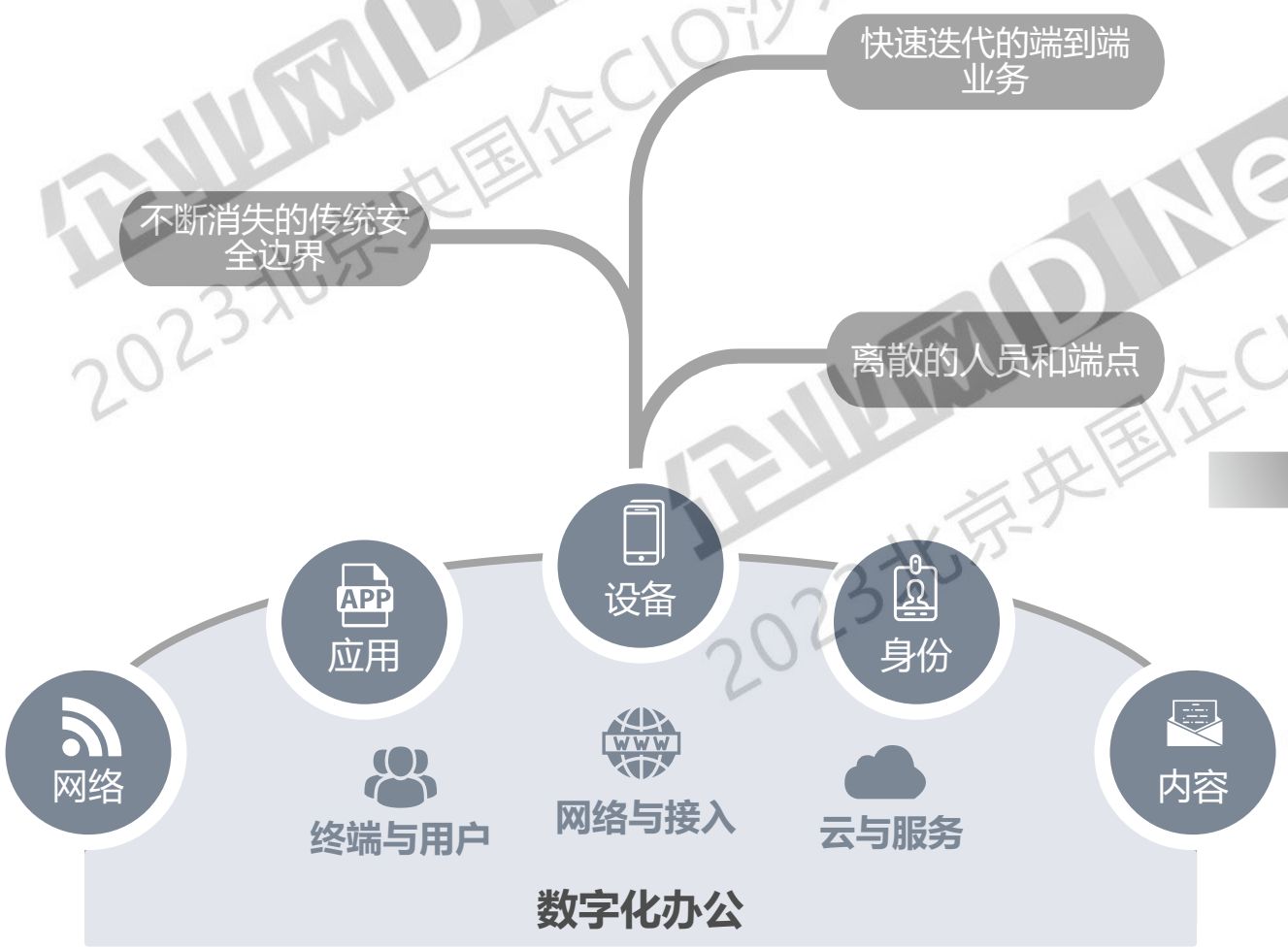
②用户身份如何保护

恶意用户通过用户账号进行仿冒，非法获取业务数据及篡改业务权限

①终端数据如何保障

办公业务数据如何在办公电脑终端和个人移动终端保障数据安全性和减少数据泄露风险

企业数字化转型面临挑战-“见管信用“



企业数字化转型中面临诸多挑战

01 见 知问题
日常数字化工作中究竟具体发生了什么?

02 管 控问题
数字化的业务是否有得到有效的管理?

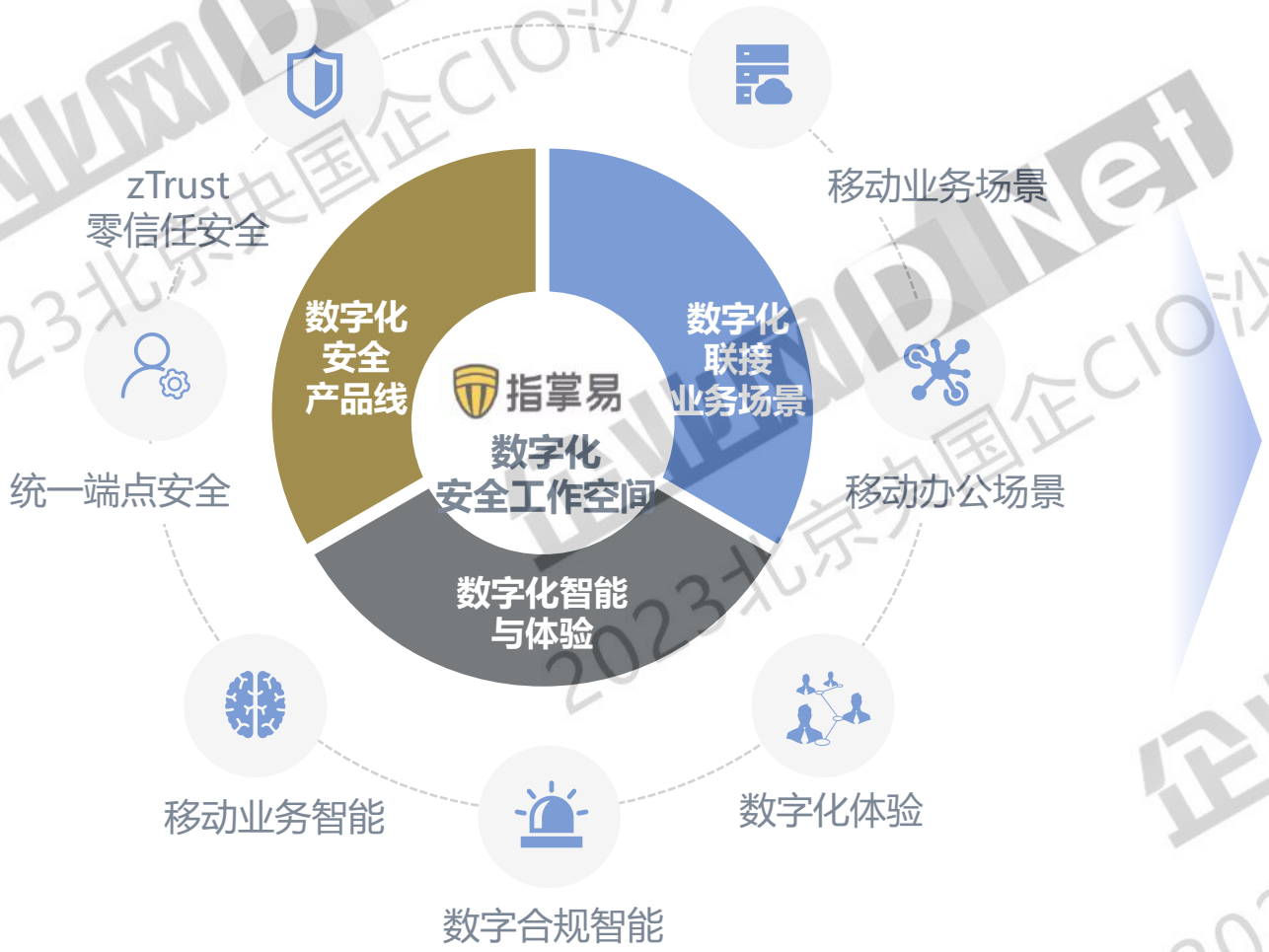
03 信 任问题
如何管控数字化工作环境的安全风险?

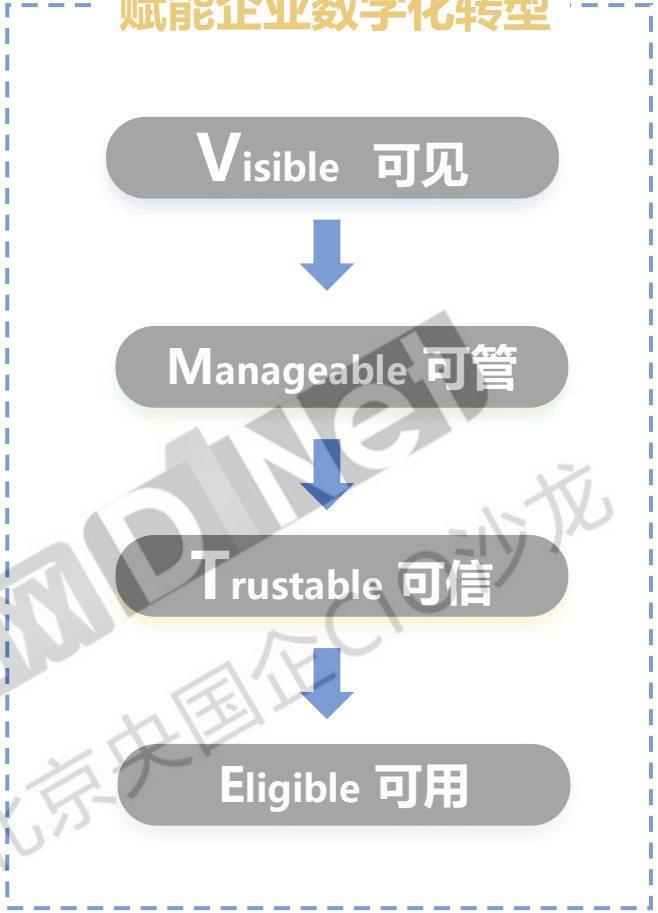
04 用 途问题
如何充分利用数字化打造业务能力?

PART
02

数字化安全工作空间解决方案

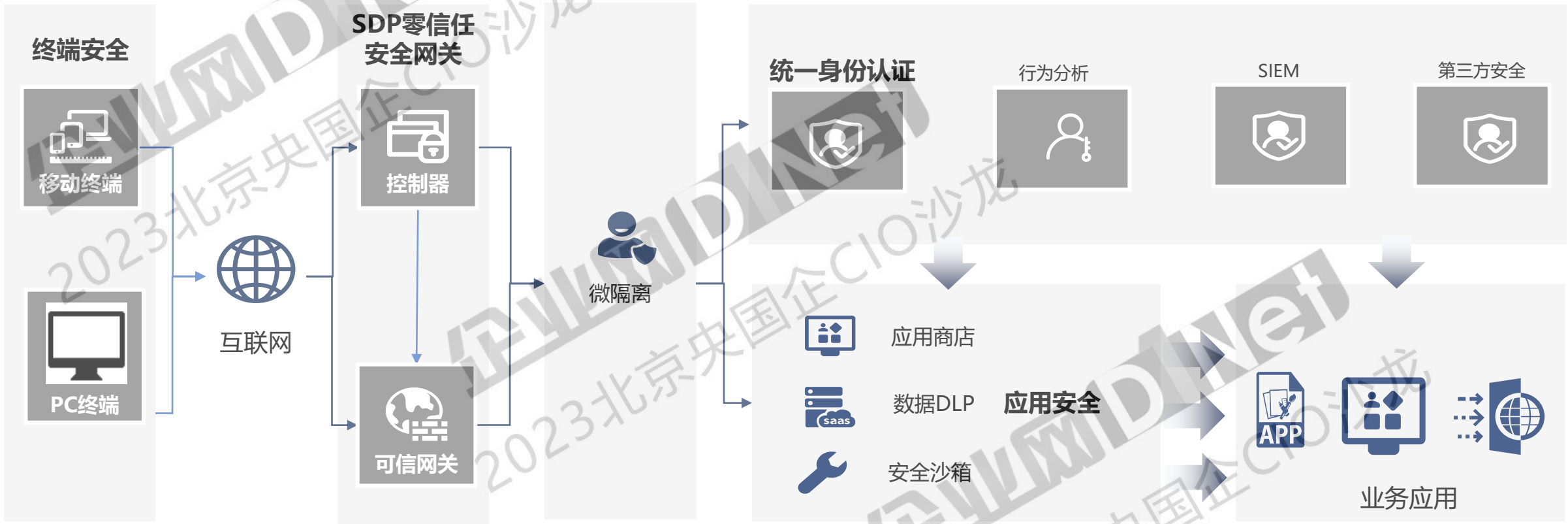
场景连接+安全产品+用户体验，构建数字化安全工作空间，赋能数字化转型





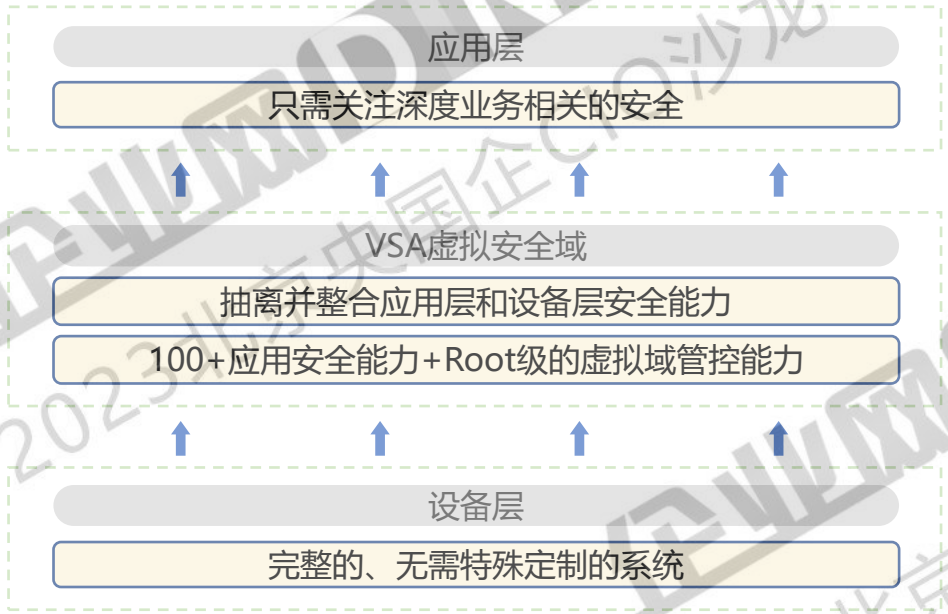
数字化安全工作空间解决方案（端管云一体化）

指掌易



移动沙箱　PC沙箱　**核心技术**　安全技术　微服务架构

主流技术：采用零信任及沙箱技术，符合主流且更具特色



易用
- ✓ 不改变使用体验
- ✓ 不影响手机性能
- ✓ 不牵涉个人隐私

敏捷
- ✓ 分钟级安全赋能
- ✓ 应用零代码改造
- ✓ 高度可扩展性

普适
- ✓ App 兼容性高
- ✓ 支持全终端
- ✓ 广泛机型适配性

SDP软件定义边界技术
- 采用UDP连接，解决TCP连接造成的DDoS及其它威胁攻击
- 安全通道使用UDP封装，不使用时不消耗资源，性能更高
- 细粒度访问权限控制，避免横向攻击风险
- 动态风险技术，访问全链路风险检测和阻断措施

SDP应用安全防护技术
- 无客户端模式，不改变用户体验并减少应用被攻击风险
- Web应用威胁防御，水印、防复制等DLP数据防泄露能力
- 加密通道兼容国际密码算法和国密算法

移动应用沙箱技术
- 小沙箱技术，隔离性与性能更具优势
- 沙箱内应用与数据具备更高安全性和管控能力

桌面终端沙箱技术
- 本地应用虚拟化技术，以本地资源利用为主，减少网络和服务端依赖
- 轻量化桌管工具，依赖性小，安全性高，可解决个人电脑远程办公安全隐患

数字化安全工作空间核心能力

基于零信任理念的SDP整体架构，同时结合数据防泄漏的终端沙箱技术、身份认证的统一身份认证技术，按照根据访问数据的敏感程度，通过分级管理、用户动态权限、依据数据流的数据全生命周期管理原则，实现基于零信任SDP的数字化办公安全工作空间

终端安全

入侵检测、安全扫描、外设管控等功能，以实现终端数据的有效保护，流转的数据，实行安全加密，保证了数据不落地

身份安全

员工身份鉴别，先认证后连接，动态自适应访问控制”机制，保护业务系统的安全

接入安全

零信任可信访问网关架设在用户与业务系统之间，为业务系统提供统一访问入口，有效收缩业务系统对外发布的网络暴露面，减少被攻击的突破口，降低网络安全风险

访问安全

建立对应用权限申请、审批和授权的流程化管理，实现对用户统一的权限控制和管理，所有web需求访问可通过web安全网关实现安全防护

数据安全

在PC端、移动终端采用微隔离技术实现数据安全功能，实现隐私数据不落地，访问设备会被进行安全基线核查，针对核查结果制定不同的数据访问策略，分配不同密级的数据访问权限

移动设备管控，提供移动工作空间和数据安全

为企业及各行业提供派发及个人移动设备安全服务，支持主流的移动手机、平板、智能显示屏、零售终端、医疗设备及IoT设备等。

平台能力

安全工作空间
虚拟工作空间，保障工作空间内业务与数据安全

统一应用商店
提供统一应用安装入口，包括上架、下架、更新、发布等

设备资产管理
设备信息、设备状态、设备绑定、设备型号等资产信息管理

设备威胁检测
针对设备提供病毒威胁检测、破解威胁检测、入侵威胁防御等

设备权限管理
设备权限统一管理，包括设备禁用、设备外设管控、设备WIFI限制、设备USB调试等

数据防泄漏DLP
水印、防截屏、防录频、防复制粘贴、现限制应用调用、文件外发限制等

移动设备管控效果

设备管控

设备资产、禁摄、WIFI、定位、锁定、擦除、蓝牙、USB等

工作空间

数据隔离、应用隔离、网络隔离

应用商店

必装、选装应用，可自动安全和更新

水印

明水印、暗水印、应用水印、屏幕水印

防截屏录频等DLP

防截屏、录频、复制粘贴、应用调用、外发、加密等

PC安全沙箱，为远程个人电脑构建安全隔离环境

指掌易

数据防泄漏DLP

- 水印、防截屏、防录屏、数据加密、应用调用限制、应用审计、复制黏贴保护

网络准入与管控

- IP访问限制、端口限制、IP段限制、安全网关控制

应用发布与权限

- 应用权限分配、准入授权、应用黑白名单、应用发布

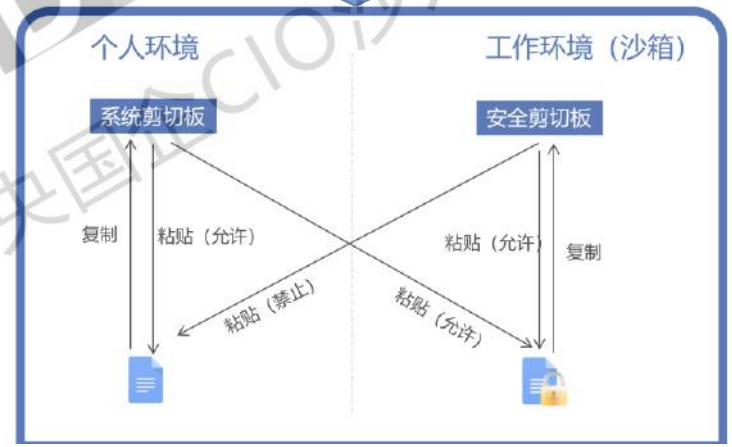
数据隔离与保护

- 外发限制、外发审批、外发审计

分析与统计

- 访问分析、日志统计、操作分析

PC安全沙箱：独立安全运行环境



PC安全沙箱效果

安全工作空间客户端
(Windows/Linux/信创)

认证登录

办公应用
(OA、费用报销、BI应用等)

DLP能力

- 水印
- 防截屏
- 防录频
- 防复制粘贴
- 限制应用调用
- 防文件转发

SDP零信任安全网关，取代VPN实现安全网络接入和访问

指掌易

软件定义边界（Software-Defined Perimeter，SDP）是一种以身份为中心实施对资源访问控制的安全框架，是零信任模型的一种实现方式，每个终端在连接服务器前必须进行验证，确保每台设备都是被允许接入的。其核心思想是隐藏核心网络资产与设施，使之不直接暴露在互联网下，使得网络资产与设施免受外来安全威胁。

单包认证

基于UDP协议的SPA单包授权认证机制，对外关闭所有TCP端口，实现无法嗅探网关端口和扫描，预防攻击行为

动态授权

根据IP、位置、时间、设备状态等异常变化，自动实现授权回收和阻断，确保最小化授权

安全隧道

采用UDP二次封装，通信隧道密钥采用高安全的加密算法，采用临时密钥机制，周期性更新，保证通信安全性

风险分析

支持持续的自适应风险与信任评估，信任度和风险级别随着时间和空间变化，自动进行信任和风险调整和应对

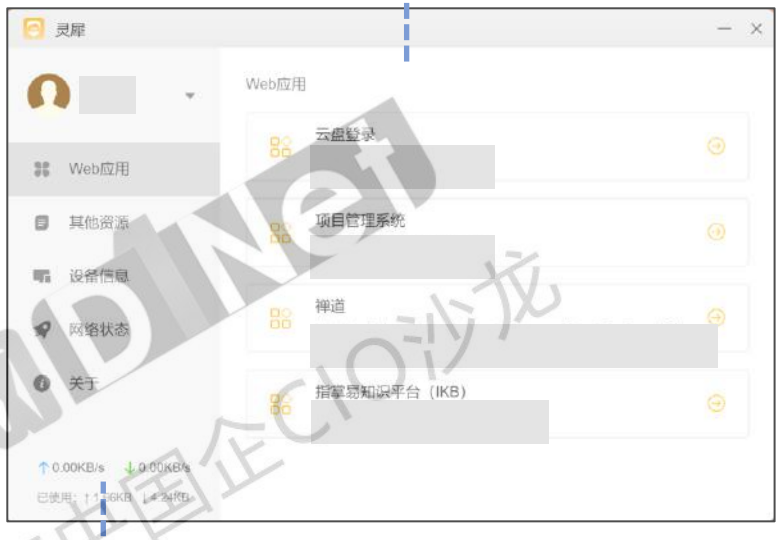
网关代理

提供应用层网关和安全策略，防御XSS、PHP攻击、远程命令执行、SQL注入等7层网络攻击，同时实现阻断

SDP零信任安全网关效果（提供移动客户端和PC客户端）

SDP客户端
(Windows/Android/IOS/Linux/信创)

访问应用



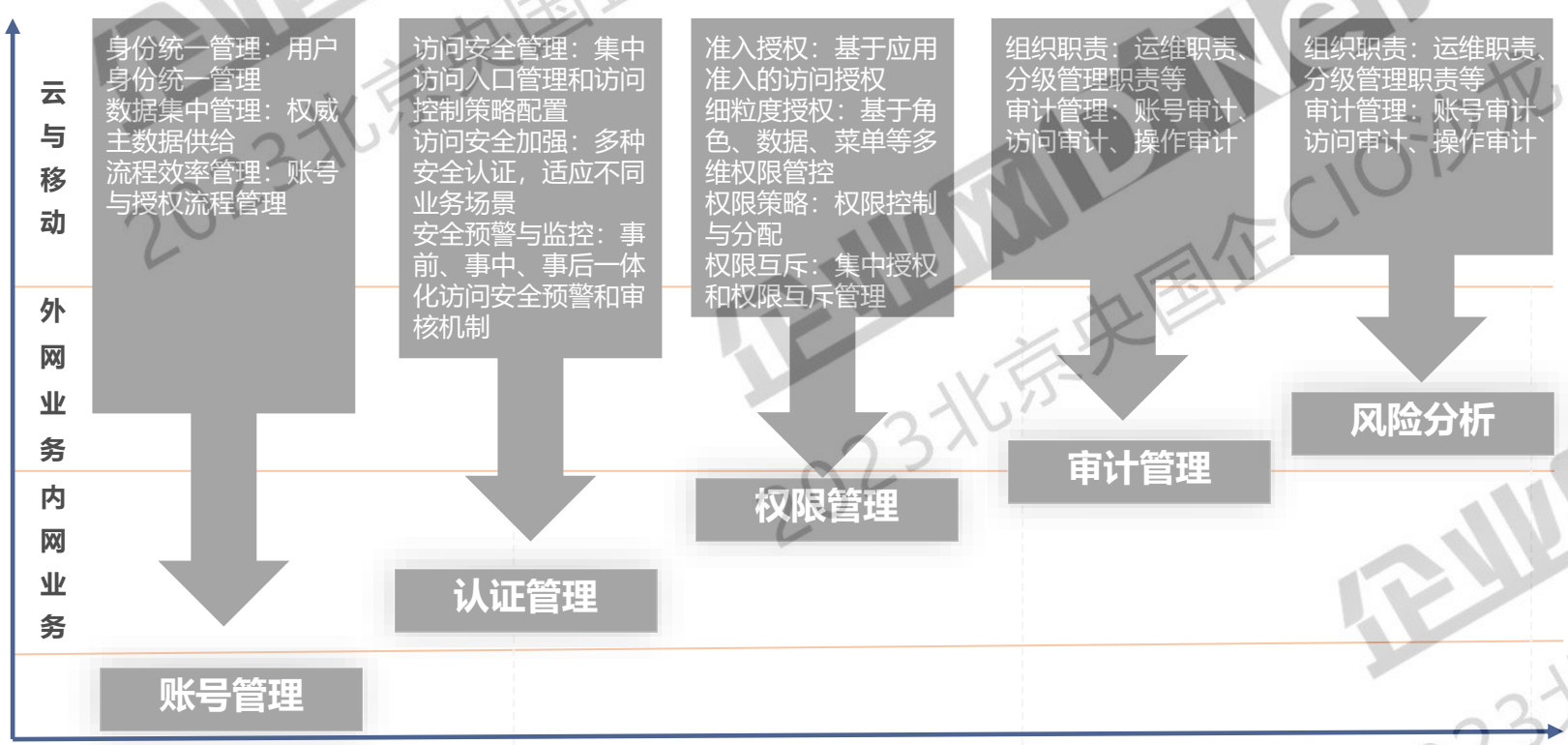
支持密码及多因素认证登录

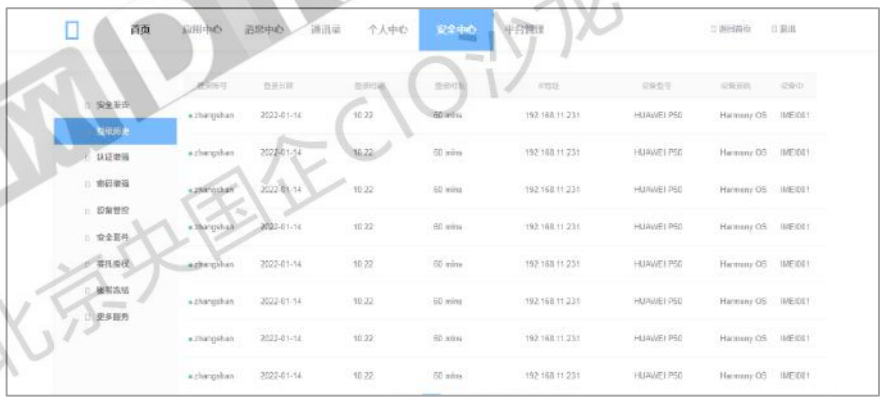
转换成内网环境

统一身份认证，实现数字化身份账号集中管理和统一认证

指掌易

统一身份认证可应用于**企业内部**、**企业外部**、**云端**身份治理，实现统一的用户账号、认证登录、权限访问、身份审计和风险分析，同时针对多元化或集团管控模式，提供集中管控，分级管控以及联邦互信管理模式和业务场景。

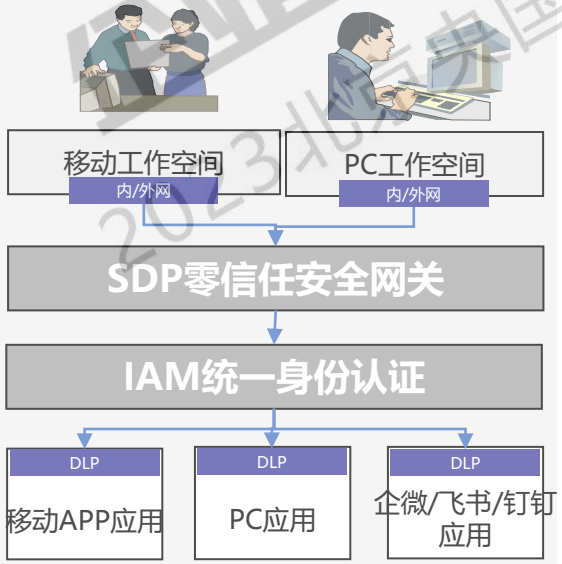




数字化安全工作空间，支撑数字化转型过程中四大业务场景

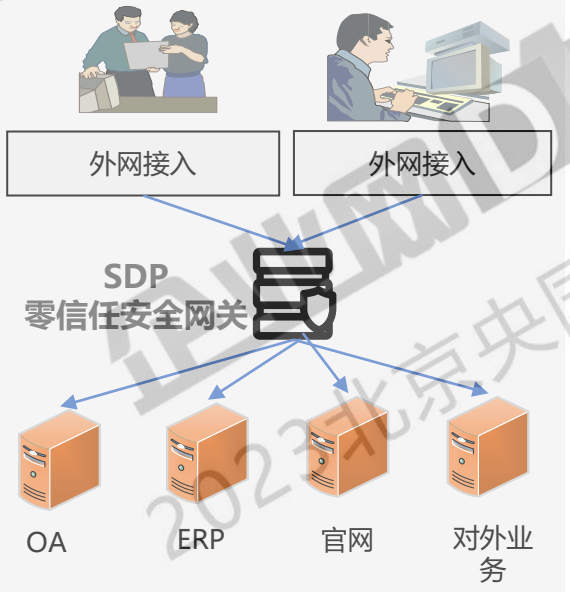
指掌易

①数字化混合办公



企业**内网办公 、远程办公、居家办公**，以终端安全、网络安全和应用安全支撑混合办公

②互联网业务收敛



企业**渠道应用、业务上云、对外业务**，以零信任SPA技术实现互联网隐身能力，从根源上杜绝网络安全攻击事件的发生

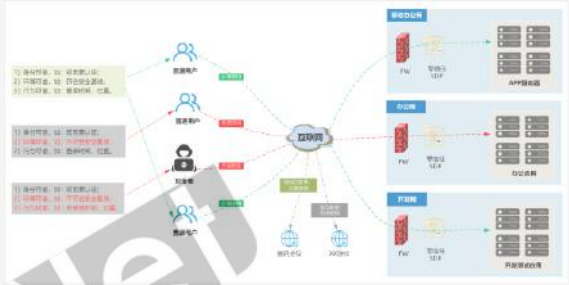
③终端数据防泄漏

数字化工作空间：数据隔离、网络隔离、应用隔离

数据防泄露DLP：防截屏、录频、复制粘贴、水印、数据加密、应用调用限制、数据外发限制、上网行为限制、数据加密传输等

企业**文档流转、人员流动、数据保护、远程运维**，以终端安全工作空间，结合沙箱技术，实现数据防泄漏

④安全测评合规



安全策略

1）用户登录双因素认证；

2）设备接入使用时间、位置在常用范围内；

3）设备绑定，默认配置1人移动和PC各1台，启用用户强制下线、超时自动下线；

4）用户登录成功后，互联网隔离，仅允许访问白名单域名；

5）保障期间不允许用户随意更换设备登录使用；

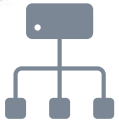
6）客户端受限分发，指定位置提供下载获取。

数字化安全工作空间业务价值

指掌易

风险降低

通过零信任安全系统的新型访问技术和防护技术，可有效减少被攻击和入侵的风险，解决VPN传统防护方式无法解决的威胁攻击，如DDoS攻击和流量攻击等



成本节省

对比传统VPN硬件形态的交付方式，一个节点一台硬件设备，成本较高，零信任安全系统采用软件交付，一个节点可以覆盖整个区域，成本可大幅节省

性能提升

相比传统VPN采用长连接访问方式，其性能容易因为被网络抖动产生不稳定情况，零信任安全系统，其网络带宽的利用率能更高，用户访问速度能更快

体验提升

用户在使用的过程中，其稳定性及用户报故障机率将大幅降低，同时采用ONEID登录方式，用户体验可进一步提升

高效运维

采取集中式的运维管理和简单的安全策略配置，减少传统端到端及各分散式节点故障带来的运维工作量，实现高效运维

PART
03

数字化安全工作空间案例实践

央企国企典型客户

指掌易

企业

中石油　国家电网　广州供电局　国家电投　中国南方电网　云南省公路局　上海铁路局　山东航空　东方航空

圆通物流　海信集团　三一重工　上汽集团　东风汽车　广汽集团　丰田合成　通力电梯　京东方　友达光电

赛科石油　金赛药业　泸州老窖　滴滴无限　伊利集团　五粮液　金光纸业　安井食品　南山集团　万科　我爱我家　美房网

宁德时代　TCL集团　中广核　深圳市机场　荣耀　传音控股　麦克韦尔　鹏鼎控股　德赛西威

贝特瑞　胜宏科技　屈臣氏　太古可口可乐　喜茶　影儿时尚　维珍妮　人人租

谢谢观看！

北京指掌易科技有限公司

400-898-7798

指掌易科技

info@zhizhangyi.com

北京市朝阳区北苑路58号航空科技大厦7层