办公安全对象是办公，应该围绕着办公工作流展开。跟围绕着公司员工。以及办公系统。以及办公区域内的网络主机等。

办公安全的建设理念有零信任。

办公安全可拆分为办公环境安全、办公系统安全、办公工作流安全、员工安全。

环境安全包括办公终端安全及办公网络安全。

办公区网络安全：

办公终端安全：EDR，防病毒，零信任终端软件，DLP等

办公系统如oa，邮箱等系统安全。财务的ERP系统，运维的jenkisn，zabbix等系统。

权限安全：管理混乱忘记删除，IAM统一认证，软件硬件认证统一认证。专用设备。

操作审计，权限审计，弱口令，渗透测试，应用安全。安全配置，安全使用。系统升级，漏洞情报。

GitHub监控，gitlab操作审计。

工作流安全：偏安全管理，比如资产申请，权限申请。应有工作流规定，不能瞎搞。特别是对于自动化的工作流，要有审批节点，通过节点管控自动化进度。

工作流：权限申请，资源申请，数据申请工作流。异常发现及处理的工作流（应急）。

员工：安全意识培训，部门培训，系统使用安全培训

在信息化/it化建设中，在IT的边界，会存在线上行为及线下行为的过渡过程。

在过渡过程中出现办公安全问题。

工作流应是制度制定方面的工作多一些。主要解决先干什么后做什么。

再就是发现不合适的线上线下过渡行为。

安全意识培训，解决办公安全问题。

保密，内鬼，内审内控，解决办公安全。

资产的安全管理，应当放到办公安全这里。

权限管理，IAM

上网行为审计

网络环境安全：纯净的网络环境，没有恶意用户接入，能发现恶意流量，阻止恶意流量。

办公系统安全：系统只有员工能使用，IAM，认证。系统安全配置。系统放在内网，服务用内网IP启动

权限安全：管理混乱忘记删除，IAM统一认证，软件硬件认证统一认证。专用设备。

办公终端安全：EDR，防病毒，零信任终端软件，DLP等

终端软件管理：

<https://www.ibm.com/cn-zh/topics/uem>

jump server + 服务器密钥

服务器安全组规则设置只能jumpserver登录

审计安全组规则，

审计所有ECS是否使用了规定的安全组

权限，行为，密码，审计。管理。

通用场景，应设置钉钉审批流。

非特殊场景，邮件审批就可以了。

从身份来讲，我们主要关注员工在入、转、调、离等各个办公周期环节中，员工权限如何能够去跟身份快速匹配。在这个点里，很多企业在人员权限变动时，更改相关策略，常常发生错配、漏配的问题，最后导致了数据资产的外泄。

另外，员工在使用过程中也需要相关的业务保障。比如分时段上很多业务系统后，每个系统都会有单独的用户名跟密码。那如何把账号进行统一管理，让员工快速触达，然后提供相关的安全保障策略？这块在身份安全管理的角度下，也是非常重要的一个问题。

第二是网络侧，目前权限的运维，包括给员工提供多种网络的接入，对于网络运维部门，存在很多的挑战。因为网络的安全、人员的快速接入以及效率，这些之间要如何平衡？

第三是终端。刚刚提到过字节跳动当年遇到的一些问题，包括现在很多企业也同样遇到了。比如说我们有个企业客户，每个电脑上有四个端，网络准入、防病毒、虚拟专用网络、数据防泄漏，各有一个客户端，这对企业IT部门，包括网络安全、运维部门的压力是非常大的。现在他们非常想把相关产品进行整合，当然也在考虑怎么去过渡。

另外是移动端相关方案的缺失。一些企业移动性管理（EMM）方案在初创型、发展型的企业里面，落地其实是比较重的。那如何能够做到多个端的安全期限能够去统一。比如说有iOS、安卓等移动办公设备需要具备一定的安全防护手段。那这个时候，我们就可以去使用比如飞连这样的轻量化产品，去适合企业当前阶段的移动安全建设。

发展阶段

SSO：

1、解决用户体验问题

2、无特定类别的用户

3、实现一点登录，全局进入。无访问控制能力

实现统一账号管理，可以解决离职-增删账号问题

4A（Account、Authentication、Authorization、Audit）

1、关注用户、认证、权限和审计

2、面向内部员工、具备人员生命周期管理

3、具备用户登录时的访问控制

4、关注权限统一管理

5、用户身份变化和访问信息记录后可以事后审计

实现基本安全管理及技术

IAM

1、面向员工、合作伙伴、顾客、设备、应用、特权账号、物理设备等，实现全生命周期管理

2、实现Service All In的单点，将B/S、C/S不同类别的应用，不同浏览器访问的统一纳管

3、实现应用级别的细粒度权限、AP操作、数据权限统一管理

4、访问控制从静态转向动态，具备实时风险发现机制和风险闭环管理能力

1. 实现身份能力的云服务化，增强用户隐私管理

更细粒度的安全管理