Enterprise Intelligent Identity Management Trend Report

企业智能身份管理趋势报告

安世加 MEGVII 旷视

2023年02月

版权声明

特别鸣谢

按姓氏拼音顺序排序

孙琦　Caspar　Chelsea Huang　Gavin Huang　Jed Wu　Karen　Lee　William Wu　蔡卓炜　曹昉赫　曹靖　陈斌　陈俊旭　陈琦　陈争光　楚春鹏　孙大川　大毛　大雄　范金成　房明宇　冯启东　顾栋　顾佳敏　顾伟博士　华树嘉　黄施宇　霍炬　金佳华　金毅　李森　李逸　廖超豪　刘敏　刘光明　刘家华　刘剑峰　刘巍　刘永杰　刘元　罗喆帅　潘浩　潘星宇　曲威凝　汤磊　田陆峰　田夜明　王思涵　王韬　王真　王子龙　夏子钦　肖森林　肖文棣　许琛超　徐猛　薛勇　杨禾穆　姚二刚　叶琳　张宏　张杰　张鲁　张勇　赵国玉　赵会强　赵磊　凝小小　朱春龙

感谢以上来自各大企业的安全负责人及资深安全专家，对此报告的大力支持！

卷首语

本报告聚焦企业智能身份管理，以身份认证为切入点，深入了解当前各行业身份管理现状，从身份认证技术，身份管理方案，到成熟落地案例，帮助企业更加全面了解如何构建身份安全体系。

—— 安世加

身份安全，既是企业运营的坚实基础，也是企业 IT 管理的核心底座。一旦出现问题，不仅将导致企业的直接经济损失，甚至还会造成品牌荣誉受损、用户信息泄露等一系列严重后果。未来，企业的 IT 管理，将以“人员”为核心，覆盖企业运维的全场景。一方面，要对“操作系统、云端应用和 IT 基础设施”施行全要素管控；另一方面，还需提前布局“数字空间和物理空间”统一的企业身份管理方案。

—— 旷视科技

序言

身份认证是对用户身份的确认，是业务层面的一道防线，也是网络安全的第一道防线。

现在主要身份认证都是多因素的认证方式：账号+密码+验证码，其中账号和密码是区别人、验证码是区别机器。区分不同人的方式有：账号+密码（手机验证码、OTP 动态口令、U 盾等）；区分人机的方式有：字符型验证码、复杂图形拼图、滑动拼图、文字点按+拼图等；也有使用新技术人脸识别等，但这些新技术也存在相关风险，比如（1）采集数据可能存在接口劫持导致数据泄密；（2）数据传输期间可能会出现数据包拦截替换（3）检测时可能会被 AI 技术照片、仿冒面具等等欺骗人脸识别，使算法失误。防与攻的未来主要点是在算法（加密、识别）的对抗上。

—— 黄帅

企业身份认证严格意义上是一个零信任实践过程，关键是将人与料一一对应并赋予动态能力。从实际的路径出发，我理解企业身份认证能分为三个阶段，第一阶段，将企业内部的 AD、SSO 等基础组件搭建起来，并结合应用系统落点到具体用户身上，实现静态身份认证的过程；第二阶段，重点在于构建 IAM、PAM 等核心平台，实现用户或组织身份的权限颗粒度细化，并伴随身份认证生命周期管理；第三阶段，通过引入信任引擎，结合基础组件、核心平台，构建企业身份认证生态，实现更为精细的权限控制并赋予动态身份认证过程，构建身份认证的零信任或有限信任状态。

—— 孟翔巍

身份认证的难点在于“最常用的密码认证并不是一种对人类友好的方式”。人倾向于记忆简单有规律的信息。即使规定了密码复杂度策略，人们也习惯使用“勉强符合复杂度要求但依然容易被猜测到的密码”。不同系统的密码需要有区别，这也加大了记忆的难度。一种解决办法是使用 KeePass 之类的密码管理工具，但管理密码文件本身也增加了安全复杂度。

从企业的角度，希望身份认证系统具备稳定的认证强度，而不依赖于员工自身的安全意识水平、记忆力或责任心等不可控因素。于是引入了 OTP 令牌、生物识别等进一步措施，但即使有了更好的认证方式，也需要保留密码作为 2FA 中的因子或前述措施失效时的备用手段。这也是与其它系统兼容所需的妥协。

我们可以看到，近几年认证的基础技术（人脸识别等）已有了很大的发展，但认证技术在企业系统中的工程化运用仍不充分，这给了身份认证厂商生存的土壤，相信随着行业的发展，未来密码认证的方式将逐渐退到次要位置，企业中的身份认证将变得更人性化、更可靠。

—— 周明昊

前言

身份认证是企业安全系体系的最基础保护，也是整个体系中不可忽视的一部分。作为安全防护的第一道防线，身份认证需要确保每个访问者的都是企业资源的合法用户，是企业安全的基石。身份认证目前已然是安全研究的重要一方面。企业的安全建设包括各个方面，但是如果在第一步身份认证就没有把好关，后续的安全部署也只能用来救火。因此越来越多企业已经把焦点聚集在身份认证方面。建设好完善的身份认证体系也是当前企业需要解决的重点，尤其很多中小企业更希望看到行业内较为成熟的案例，再结合企业具体情况来建设，省去试错成本以及增加可靠性。本次报告我们采访的企业包括制造，金融，互联网，医疗等各个行业，规模包括超大型企业，大型、中小型、微型企业，不仅收获了很多优秀落地经验，也看到企业在身份认证建设中遇到的困境。本次报告也是根据多次访谈总结的身份认证现状以及未来趋势，希望对企业身份认证管理有参考意义。

目 录

概 述

经过大量调研，我们发现基于身份认证环节的攻击，正逐渐成为各类攻击中成功率较高的一种手段，被调研的企业中很大一部分都存在因身份认证防护不到位而产生的安全问题。

我们进一步调研发现，员工使用弱密码、认证防护缺失屡见不鲜，钓鱼邮件攻击和暴力密码破解攻击等是针对身份认证环节的主要攻击手段，其呈现出攻击成本低和日益多发的趋势。大部分企业并不具备遭受攻击后的有效溯源能力，直接导致了问题从发生到被发现、被处理耗费了大量的时间，期间所产生的安全风险往往也难以估量,部分受访企业也坦诚其无法承受由此产生的数据泄露、业务中断和品牌声誉等损失，从而使企业陷入非常被动的一个局面。

制作这份调查报告的目的是希望能帮助企业了解基于身份认证攻击的威胁并帮助企业有效处理这类安全问题。借助超过 100 人次的人物访谈，我们希望为读者呈现一个非常客观和真实的观察视角。

如果你是企业的决策层，一名正在主导企业数字化转型的 CEO，你将获得非常宝贵的管理者观点，即更智能的企业身份管理能力对于数字化转型至关重要，其重要程度仅次于用数字化重构其业务主线并实现可持续的盈利。

如果你是一名技术决策者，你将获得大量同行、跨行业的技术决策者们的思维碰撞，他们对于更智能的企业身份管理能力的理解和实践方向等。

重要发现

1. 企业对于身份认证管理的认识不足

国内大部分企业在身份认证管理方面没有专项预算，大部分都是以安全整体建设覆盖，大多用于服务和设备采购。

2. 企业对于内部 IT 人员及部分权限较高的员工缺乏有效管理手段

近些年“内部员工恶意删除公司数据”事件时有发生，企业高层由于缺乏专业 IT 背景知识往往依赖行政手段预防此类问题，缺乏技术性手段的约束。

3. 企业逐渐重视身份认证管理的重要性

员工使用弱密码、共享账号屡见不鲜，身份凭证安全管理形同虚设。身份认证管理是数字化能力的基础，大部分企业已经意识到身份认证管理是企业最为重要的一项安全和管理能力。

4. 企业需要的身份认证管理能力是更为智能的身份认证管理能力

企业已有的身份认证管理手段无法很好的判断用户的真实身份，且难实现易用性和安全性的平衡。有 52%的受访用户希望在未来落地更智能的统一身份管理解决方案，将“设备、应用和系统”进行统一管理，为员工提供更易用和安全的数字化服务。

5. 企业积极拥抱公有云，混合云模式将是目前企业的最优选择

企业从成本考虑，正积极拥抱公有云服务，但其原有的大量线下资源在与公有云服务的组合中产生了大量尚待解决的问题，身份认证管理问题尤其突出，大量企业目前呈现出混合云环境中的多套身份认证管理割裂的问题，大大增加了管理成本和安全风险。

6. 未来 12-36 个月，企业不会大幅增加专业安全人员配备

由于对于未来预期的不确定增加，企业并不会考虑大幅增加专业安全人员的配备，部分企业甚至考虑仅保留最小配备的专业安全人员。

第一章

企业身份认证管理概述

一、企业身份认证管理概述

1.1 行业和企业概述

为了更为全面和客观的反映企业身份认证管理的现状，我们做了大量的企业真实情况调研，我们可以看到金融和制造业企业的参与度是最高的，这也和企业本身对于身份认证管理的迫切需求存在一定关联。

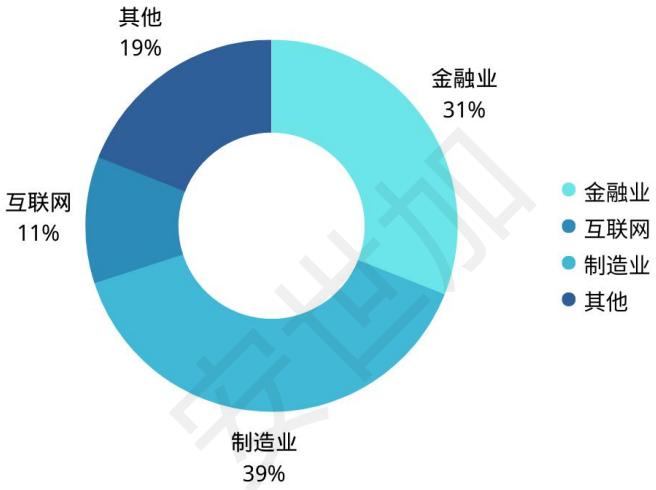


图 1　受访企业行业分布

被调研企业中，规模以上民企和国企占比较重，他们也代表着当下最为真实的数字化转型主力，他们希望在数字化转型中落地更智能的身份认证管理能力，已为其数字化转型打下坚实的基础。

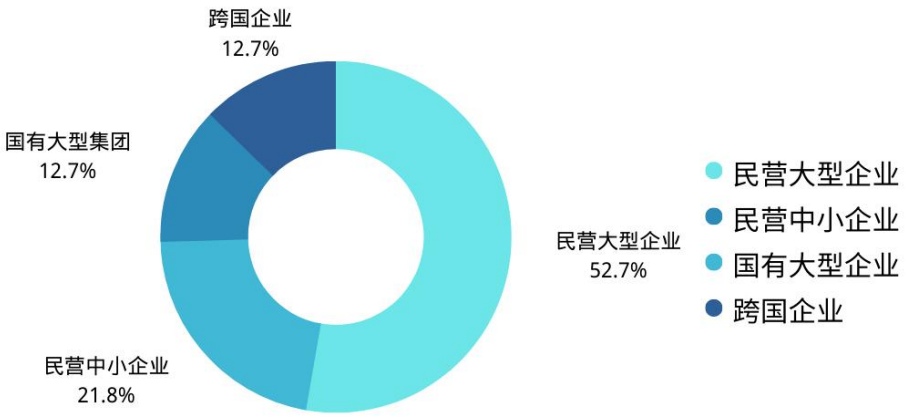


图 2 受访企业类型分布

在被访企业中，绝大多数企业的员工数量都超过了 1000 人，从侧面来说这样的超大型环境也是身份认证攻击防护非常困难的一个局面，因为任何一个点的突破都有可能面临全面的失守，部分企业坦言他们迫切需要一种更为智能的企业身份认证解决方案来帮助他们解决问题。

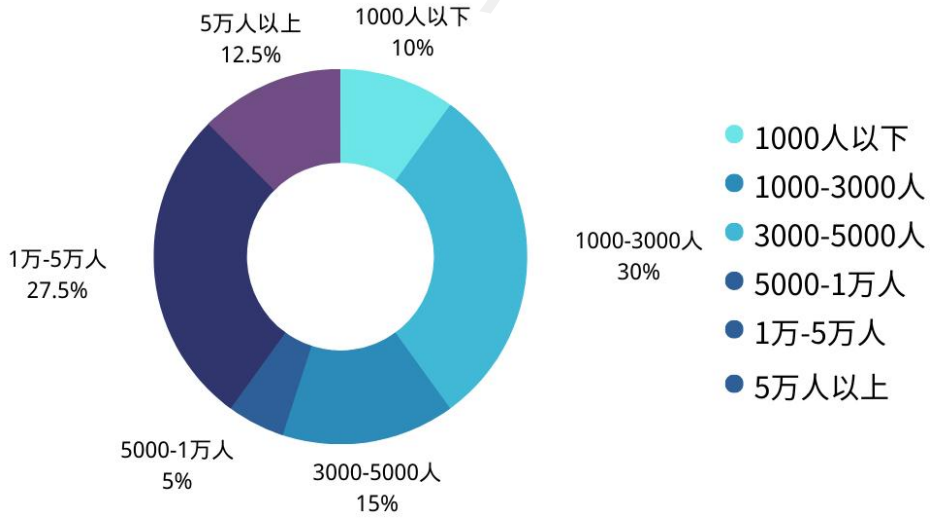


图 3 受访企业规模分布

1.2 身份认证管理技术概述

1.2.1 Multi-Factor Authentication

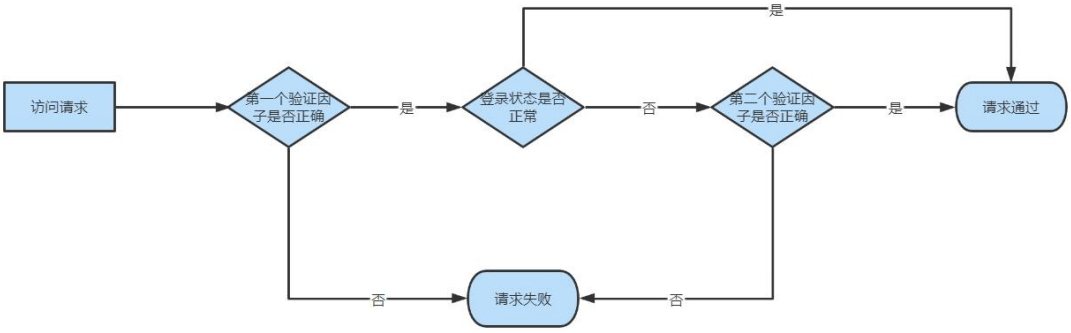


图 4　Multi-Factor Authentication

Multi-Factor Authentication，缩写 MFA，也就是我们所说的多因素认证，它是一种要求用户同时进行两种及以上认证机制后才能获得授权进行资源访问的一种访问控制手段。在我们的日常生活中已经有大量的 MFA 应用，比如你登录大部分手机银行的 App，除了你的密码外还会要你同时提供注册用户本人的单次手机登录验证码进行身份确认，在涉及大额交易的过程中会要求你输入 U 盾的验证码等方式来验证你的合法身份。这种方法目前已经被有效验证是相对安全可靠的一种手段，在条件允许的情况下我们也非常推荐大家在企业中全部推广这种访问控制手段。

1.2.2 Single Sign-On

图 5　Single Sign-On

Single Sign-On，缩写 SSO，也是我们所说的单点登录，它的诞生主要是解决用户需要在不同的应用系统中每次都需要身份验证的问题，即一个用户只需要在身份认证模块中完成身份认证后，便可用这个认证结果在不同的应用中去匹配正确的权限，完成从认证到授权使用的全过程，这样用户只需要在一个入口处输入用户名和密码后，便能自由的访问所有基于 SSO 的应用系统，极大的方便了用户，实现一套账号走遍天下的便捷。

1.2.3 Role-Based Access Control

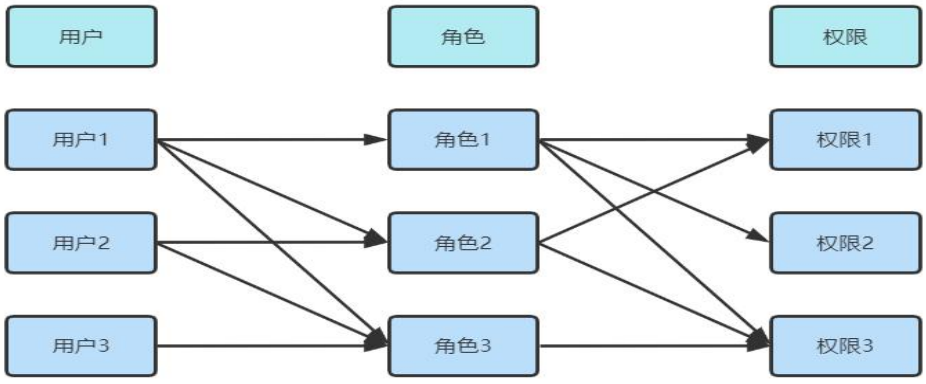


图 6　Role-Based Access Control

Role-Based Access Control，缩写 RBAC，也就是我们所说的基于角色的访问控制，它是一种非常有效的面向企业的安全访问控制策略，在涉及大量人员的场景下被充分验证其是一个非常有用的访问控制方式。它的基本思路非常简单，不针对单个用户进行授权，而是直接对用户集合（比如，用户群组、角色）进行授权，这样做的好处是不必在每次用户发生变化是都去进行权限的变更，只需要针对一个用户群组或角色进行变更就能实现对群组中所有用户的权限变更，大大的减少了用户管理的难度和系统开销。

1.2.4 Identity as a Service

企业可以使用云服务厂商原生提供的身份认证管理服务，他们称为 IDaaS，Identity as a Service，这里我们需要了解的是背后的认证和授权的技术支撑，OAuth 2.0、OIDC、SAML 2.0 和 SCIM2.0。对于这些标准协议我们不去做更多的拆解，企业可以在进行具体落地时进行评估。IDaaS 需要为我们提供如下的主要能力：统一的账号管理、身份认证、授权管理、应用管理和审计管理。绝大多数企业的自研身份认证管理服务是基于 OAuth 和 OIDC 的，如果企业是采购的云服务，你需要清晰的了解你买的服务是什么以及你需要做哪些、云服务厂商提供了哪些能力。

1.2.5 统一身份认证

统一身份认证是一套完整的供各应用系统使用的身份认证系统，用户完成登录统一身份认证服务的认证后，即可实现登录所有接入系统“一号通行”的效果。一般而言，统一身份认证是统一身份认证平台的核心基础服务之一，主要负责用户的身份、状态、权限、单点登录业务系统等相关信息的校验，通过身份认证模块和权限管理模块等组件的组合实现“一次登录，多次使用”，在提升了安全性的同时解决了账号和密码难以管理的问题。

1.2.6 零信任

Zero Trust Architecture，缩写 ZTA，也是我们常说的零信任，它本身是一种安全理念，概括而言可以理解为永不信任和持续验证，对任何进入网络的主体先行验证，再予以放行。零信任的技术栈由软件定义边界（SDP）、身份权限管理（IAM）、微隔离（MSG）这三大部分组成，明确身份管理是基础，结合最小权限原则和实时计算的访问控制策略和资源授权原则，实现基于多维度数据为基础的信任等级评估和授权，从而实现更可靠的安全能力。

1.2.7 基于人脸识别技术的身份管理

越来越多的企业正在考虑基于生物识别技术的认证方式，实人人脸验证技术因其可靠、便捷、安全的特性获得了大量关注。人脸识别技术可以与现有绝大多数身份认证系统无缝链接，特别是在一些对于用户身份验证要求较高的环境中获得了越来越多的使用占比，原本需要使用 MFA 的很多场景都因为人脸识别技术的落地而得到简化，原来需要密码加短信验证的 MFA 场景，现在只需要用户刷脸即可。基于人脸识别的免密身份认证与管理，即简化了登录流程也提高了用户的使用感受，同时由于生物信息的唯一性也提升了对于行为审计和记录的可靠性。在一些强调高安全性的场景中，通过密码加人脸识别的 MFA 解决方案也正在被人们广泛接受，相比短信、邮件、动态口令等技术手段人脸识别在安全性和便捷性等方面的优势非常明显。

1.2.8 其他

企业对于访问控制的需求正在发生变化，针对分布式系统、去中心化的认证方式、BYOD 和 IoT 等等情况，在不久的将来我们预计基于生物识别验证、人工智能和机器学习等手段将会被加入到身份认证管理的范畴，结合我们具体的业务场景为我们提供更为便捷、高效和安全的认证管理服务。

第二章

企业身份认证管理能力现状及需求

二、企业身份认证管理能力现状及需求

2.1 金融、制造业身份认证需求

我们对本次调查占比最重的两个行业——金融和制造业进行了深入的剖析，一是因为他们所在行业正在遭受日益严重的基于身份认证环节的恶意攻击；二是他们所表现出的强烈的对于智能身份认证管理能力的需求，我们相信基于大量真实需求和案例的信息将会更好的帮助我们解决与日俱增的基于身份认证环节的恶意攻击。

2.1.1 金融行业身份认证需求

银行、证券期货、保险这三个细分的金融领域对于智能身份认证能力的需求度是最高的，他们的员工规模数量也都是大于 1000 人以上的中大型企业，在这样的环境中如何平衡便利性和安全性是一门艺术，由于强监管的背景，他们早早的就具备了多因素安全认证能力，但即使是经历了多年技术沉淀的行业，他们也对于更智能的身份认证管理存在强烈的需求。

金融行业企业情况

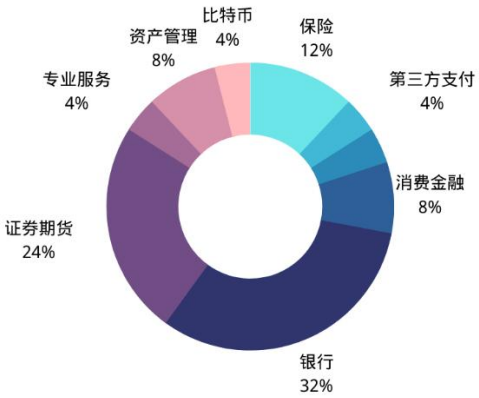


图 7　行业细分

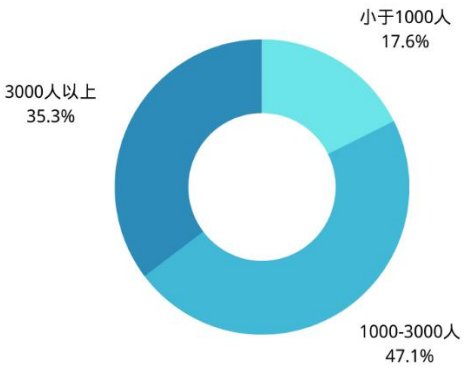


图 8　人数规模

2.1.2 制造行业身份认证需求

另一个我们重点关注的行业是制造业，汽车、电子元器件、机械制造这三个细分领域，他们的员工数量也是超过 3000 人的大型规模，伴随着数字化转型的浪潮他们正加速推进更安全的身份认证管理能力建设。

制造行业企业情况

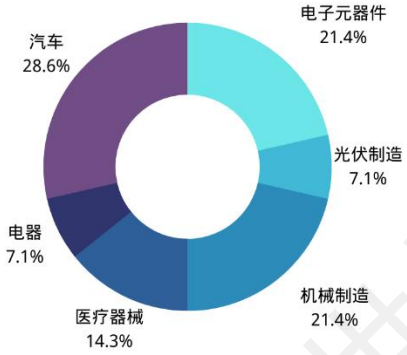


图 9　行业细分

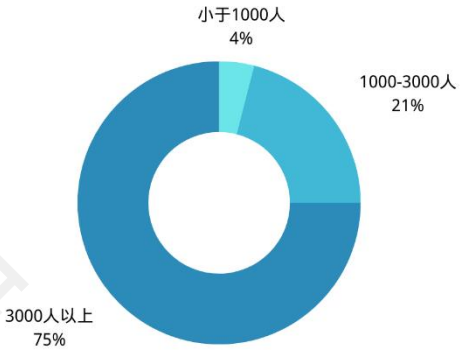
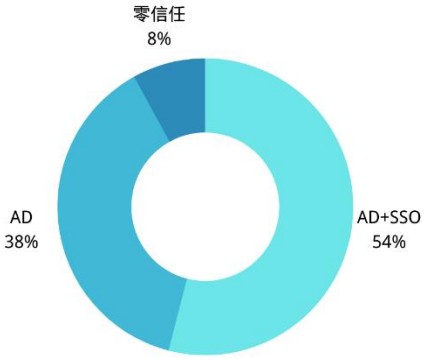


图 10　人数规模

2.1.3 绝大多数企业采用 AD 构建企业身份管理体系

我们对金融和制造业的相关企业现阶段在身份认证管理能力的情况做了细致的分析，绝大部分都基于 AD 构建了自己的 SSO 生态体系，通过 AD 实现统一的账号管理体系，通过自研+核心模块采购的方式集成 AD，最终实现企业内部的身份管理架构。这里有一个比较有意思的现象，金融行业的用户对于智能身份管理和零信任两块安全领域表现出了较大的前瞻性，部分企业已经有了成熟的落地案例。

制造行业和金融行业企业身份管理建设情况



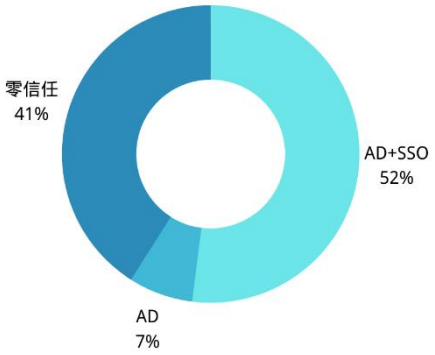


图 11 制造行业身份管理建设情况　　图 12 金融行业身份管理建设情况

在对于未来身份管理需求的访谈中，零信任和智能身份管理是比较明显的两大趋势，前者强调的是“持续验证，永不信任”，如果是一个从零到一的环境我会毫不犹豫地考虑该方案，但对于已经相对成熟的大型环境而言，巨大的改造成本使企业倾向于落地更智能的身份认证能力来提升其安全和管理能力。

2.1.4 特权账号多采用堡垒机进行管理

针对特权账号的管理也是企业关注的另一个重点。在具备了较为完善的特权账号管理体系的企业中，对于具备较高权限的特权账号的管理一直是关注的重点，超过一半的企业通过堡垒机来进行账号的管理。针对 IT 人员部署的堡垒机由于缺乏良好的用户使用体感，往往在部分业务场景中被非专业 IT 人员吐槽使用体验太差，这部分需求也被认为是企业进行全面身份认证管理能力升级的一个原动力，即让用户能够在便利和安全性之间实现最大的平衡。

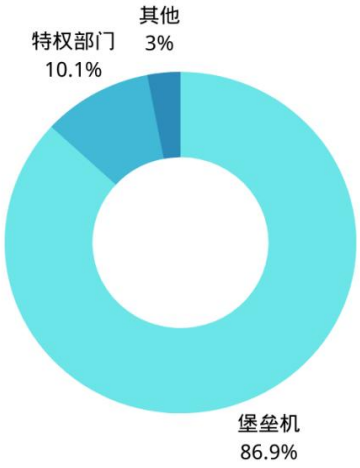


图 13 特权账号管理

2.1.5 核心业务场景中，均已启用多因素认证，提升访问安全性

调研中，超过 96%的金融企业均已经落地 MFA，特别是针对其核心业务系统基本是 100%的启用了 MFA 来进行安全加固，只有少部分边缘系统未启用 MFA。在堡垒机、VPN 等环节中使用 MFA 的比例是最高的，其次是一些基于 SaaS 的业务系统、邮件系统等。在问及是否会全面启动 MFA 的落地时，大部分被访者都是希望能够有一套更智能的身份认证系统能协助其完成基于 MFA 的企业身份认证管理能力升级，最重要的是要兼顾易用性和安全性。

多因素认证使用场景分布图

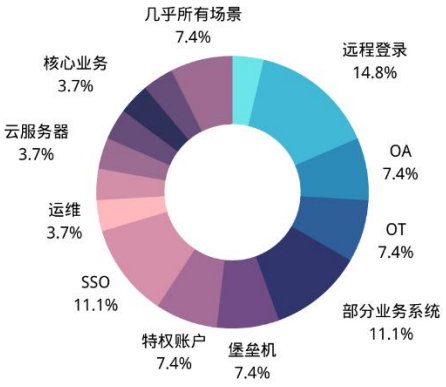


图 14 制造行业

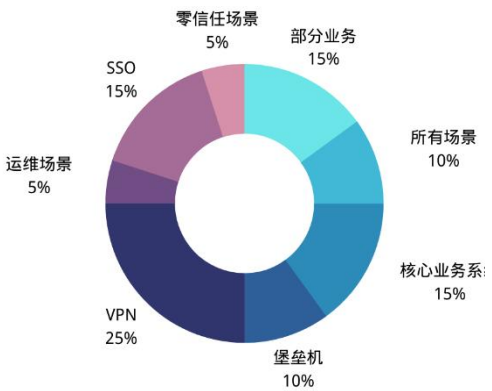


图 15 金融行业

在有效的 MFA 场景中，手机令牌和短信验证这两种方式占据了绝大多数的份额，这也是目前在日常生活工作中最为常见的 MFA 方式。近年针对短信钓鱼和中间人的攻击也使大家逐渐对短信验证的安全打了一个问号，短信服务商是否有足够的安全能力和手段去保护这些重要的安全信息？运营商是否能确保短信的安全？在特定场景下无法接受短信时的不便等等，让部分用户开始尝试使用诸如人脸识别的新的 MFA 手段。

多因素认证方案种类分布图

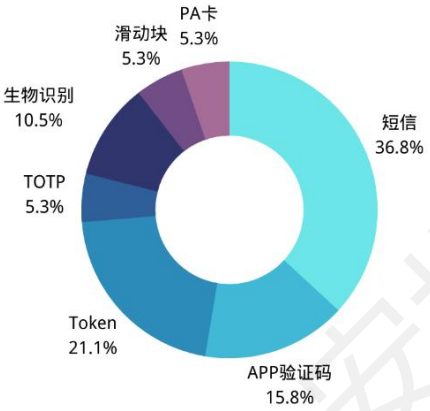


图 16 制造行业

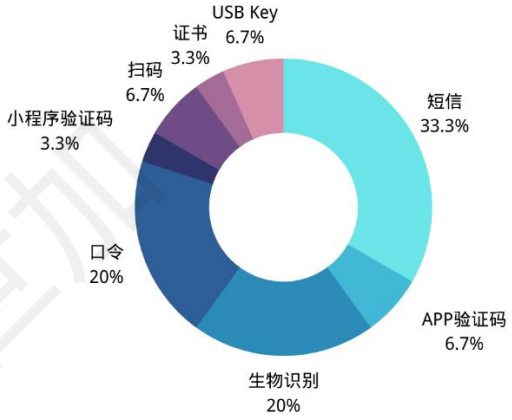


图 17 金融行业

2.2 生物识别技术在企业办公场景下的应用情况

2.2.1 部分被调研企业已采用人脸识别技术，提升身份认证管理安全性

针对上述提到的部分用户考虑使用生物识别作为 MFA 的手段，我们进一步分析了人脸识别等生物识别技术的实际使用情况。被访企业中，有部分企业已经落地了人脸识别场景，“更高的安全性”是其看中的最重要因素。在核心系统、生产系统、特权账号、共享账号管理等环节，通过采用人脸识别技术，有效提升了身份认证管理的安全性。部分企业在落地 SDP 的时候也同步启用了人脸识别作为其重要的日常运营和安全管理的基石。

办公场景中生物识别使用情况

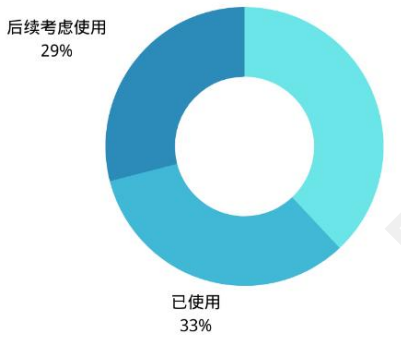


图 18　制造行业

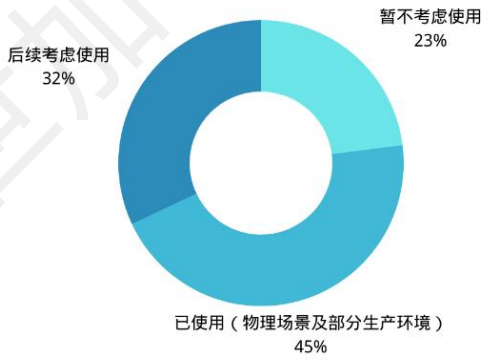


图 19 金融行业

2.2.2 投入不足或无安全事件驱动，生物识别技术被延迟部署

对于其他暂未部署生物识别技术作为 MFA 手段的企业，最主要的原因是预算不足或企业目前没有需要落实生物识别的高级别安全场景。我们可以理解在企业整体的安全边界内必然是基于业务的重要程度和安全级别综合考量应用各种管理手段的，部分被访企业的安全负责人也坦言目前主要的问题是企业在安全投入不足，导致其首要目标就是聚焦于最核心的那部分数字

资产，对于其他重要但不紧急的事情只能先搁置一下，通过其他的次级安全措施来尽可能的确保其安全运营。

部分受访对象坦言，在预算充足的情况下他们将全面启用基于生物识别技术来代替现在正在使用的各种 MFA 手段，如短信、邮件、动态口令等。在用户使用体验上，生物识别技术的体感无疑是最佳的，正如在 iPhone 等智能手机中启用了人脸识别后，绝大多数使用者都不会再去使用密码或者指纹等身份识别手段。在企业的 IT 环境中，也存在一样的内在需求，企业的 IT 部门迫切需要一种能平衡高安全性和良好用户体验的技术手段来帮助他们提升用户满意度。

合规隐私风险是一个大家都高度关注的焦点，需要公司层面的法务和行政部门一起介入才能有效地一起推动人脸识别技术的落地。人脸识别技术本身是安全可靠的，我们在企业环境中如何框定它的使用范围、使用区域和使用方法都是我们需要特别注意的。我们发现在已经落地的企业中往往都是通过约定明确的使用场景和使用方法，向员工提供两种以上的技术实现手段并充分尊重员工的选择权后，员工会逐步从一开始的犹豫逐步过渡到选择更为便利和安全的人脸识别技术场景。

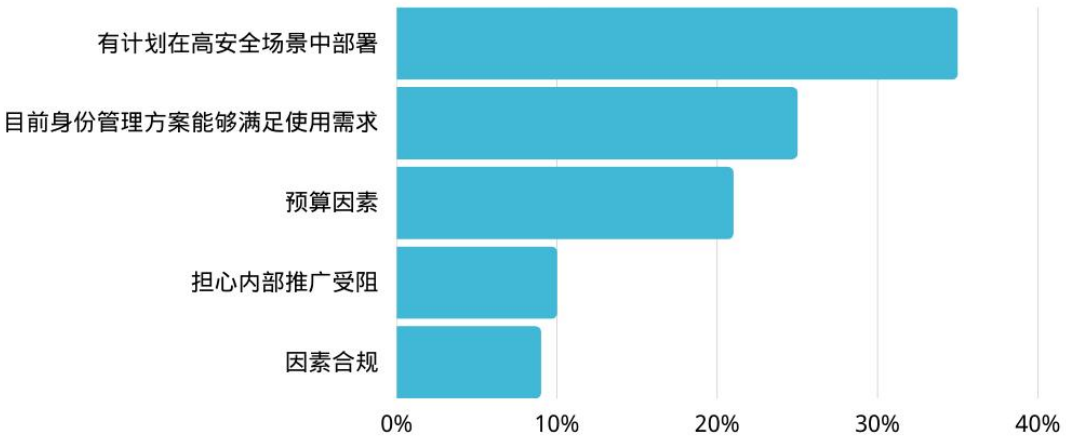


图 20 未部署生物识别技术的原因

2.3 云服务的使用

我们非常欣喜的绝大部分企业都有了其身份认证管理能力，线下环境中大部分企业都基于AD 构建了自己的身份认证体系，混合云环境中大部分企业存在身份认证割裂的问题，即某一领域中使用一套身份认证体系，在另一个领域中使用不同的身份认证体系。这个问题产生的本质是由于业务发展导致的新系统以超乎想象的速度融入企业当下的数字化环境，其本身自带的一套身份认证体系未能很好地融入企业原有的身份认证体系，有技术原因也有管理因素，我们针对被访企业的云服务使用情况也进行了一次调研，希望能够更多的了解企业在步入数字化转型深水区后在复杂环境下的身份认证管理之痛。

企业基于成本考虑，正在加速对于部分业务上云的尝试，特别是一些体量较轻、相对独立的一些业务，云服务相对灵活的计费方式正好满足了企业的需求。在我们的调研中，大部分企业都采取了前端上云+后端本地的方式，即将数据存储保留在原有的数据中心，把应用部分直接放在云上，企业希望以较低的试错成本和确保数据安全的角度来进行一些真实业务活动上云尝试。

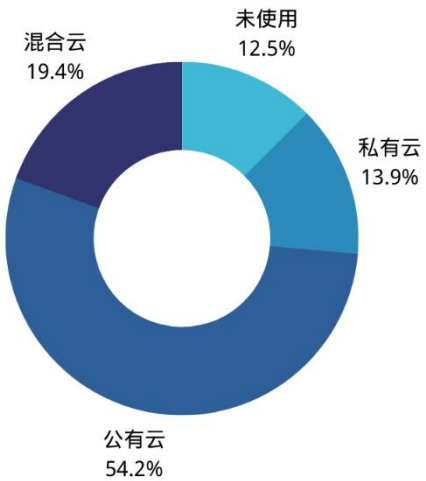


图 21 云服务使用情况

云原生服务本身自带一套身份认证体系，有超过 1/3 的企业使用了云厂商自带的身份认证体系，还有超过 1/4 的被访企业将其身份认证体系纳入了现有的堡垒机进行统一管理。不同类型组织在混合云环境下对身份认证管理的能力呈现出了较大的差别，跨域的统一身份认证需要有一定的技术能力作为支撑，这也是部分大部分企业在混合云环境下采取了多套身份认证管理的原因。

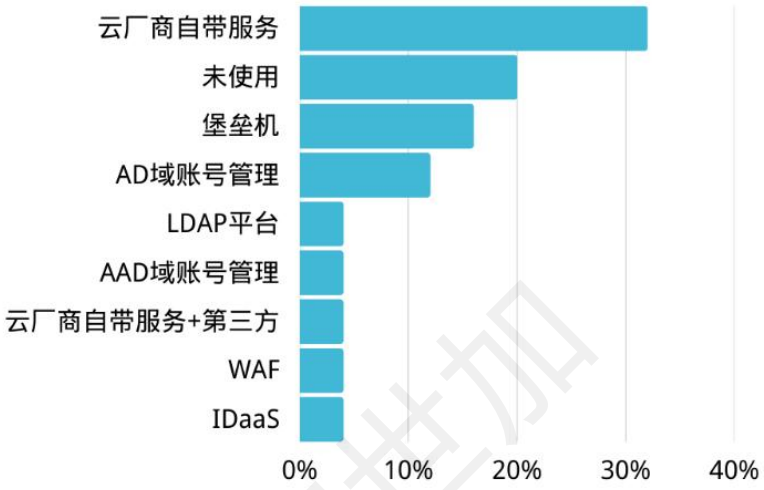


图 22 云上业务身份管理

2.4 零信任技术的使用

零信任也是当下一个非常火热的理念，它的理念是永不信任和持续验证，对任何进入网络的主体先行验证，再予以放行。企业选择零信任的主要驱动力是更高的安全性和升级现有远程办公体验，软件定义网关（SDP）和微隔离（MSG）等技术都有望能满足企业的这部分需求。超过 46%的被访企业表示，他们已经启动或者计划在未来 1-2 年的时间内实施零信任建设。特别是金融行业，超过 60%的被访金融企业已经启动或者计划在未来 1-2 年内实施零信任建设，制造业有约 46%的企业因为预算、业务影响严重等因素而放弃零信任建设。

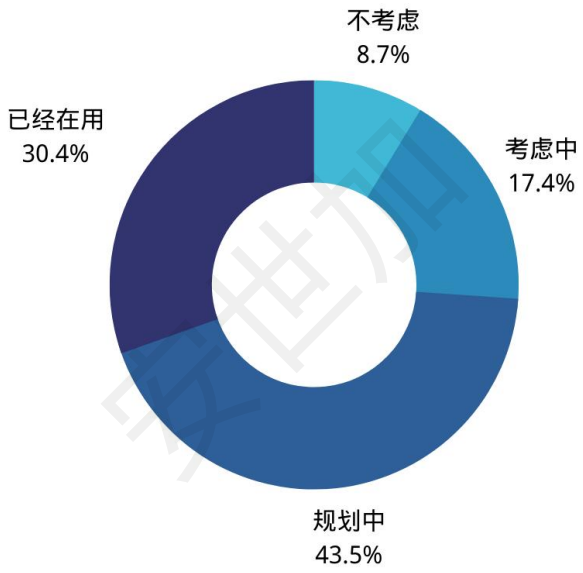


图 23 零信任建设情况

第三章

新一代
企业身份认证管理需求

三、新一代企业身份认证管理需求

3.1 传统身份认证方式面临诸多挑战

- **管理成本高昂**

基于传统 AD 或 LDAP 等技术的身份认证管理手段有较高的技术门槛，且其顶层架构设计的好坏将直接决定其日常运营成本的高低。

- **安全挑战巨大**

办公、IT 运维、远程接入等场景中，员工使用弱口令、共享账号等问题一直困扰着企业的身份认证管理工作，同时以盗取身份凭证为目的的，钓鱼攻击、暴力破解攻击防不胜防。证明“你是你自己”的伪命题却真实的发生在恶意攻击的场景中，直接导致严重的安全事故。常见的多因素认证方案，如短信、邮件、H5、小程序令牌，应用扫码或者 USB-Key 等方案，都存在凭证被劫持盗用的风险，无法确认是本人操作。

另外，随着信创建设进程加速，国外设备、管理系统逐步淘汰。企业身份管理平衡将会被打破，企业需要对信创设备和系统、现有 IT 系统进行标准化统一管理。

- **用户体验不佳**

用户面对一堆账号和复杂密码根本无从下手。在严格的密码策略下，员工设置密码时既要设置大小写，又要 2-3 个月改次密码，还要确保新密码和前几次的密码不同，业务部门怨声载道。同时，传统 OTP 方案，比如短信、邮件，信息经常存在延迟现象，认证超时导致的重复操作也时有发生，严重影响办公效率。

- **管理面临挑战**

普通员工账号的管理以及高权限的特殊账号管理是企业 IT 运营的一大难题，随着企

业规模和组织架构的变化，这一管理难题将进一步凸显，管理手段急需升级。

如今，企业内部共享账号很多，但无法确认登陆者的真实身份，一旦发生运维事故，很难确认最后一次敏感操作执行人的身份。此外，由于第三方运维人员更换较为频繁，许多运维管理账号的交接无法有效管控，长期不使用的特权账号成为僵尸账号，并有可能被离开的第三方人员利用。种种安全隐患，导致身份管理形同虚设。

- **合规监管要求**

国家层面推动的信创工程进一步要求金融、制造、能源等行业企业，尤其是国央企企业，采用自主可控产品方案。但更新换代后的信创系统、信创设备的身份管理问题依然存在。促使企业加快信创环境下的新一代统一身份认证能力建设。

传统的基于 AD 或 LDAP 等技术手段实现的身份认证方式，在经历了长时间的发展后已经充分地证实了其稳定性和可靠性，能够满足企业传统意义上的身份认证管理需求。但在当下企业追求全数字化转型以及数字孪生的大背景下，传统的身份认证方式的弊端也逐渐显现，安全性相对较弱、用户友好度较低、管理成本高昂和灵活性不足等弊端限制了企业的发展，企业希望有一种兼顾良好用户体验和充分灵活技术的身份认证解决方案，帮助企业重新打造以身份为管理核心的新一代数字化综合能力。

3.2 新环境下的身份认证管理需求

企业所面对的是一个整体安全面的威胁，他需要 360°无死角的覆盖才能形成有效的安全防护能力，受限于管理层安全意识较弱、安全预算不足、业务配合度底等问题，企业的信息安全能力建设与其业务规模存在一定的落差。企业的安全负责人主动转而聚焦在企业身份认证环节，希望通过更智能的企业身份认证能力来将夯实企业数字化能力的第一道防线——身份认证管理。

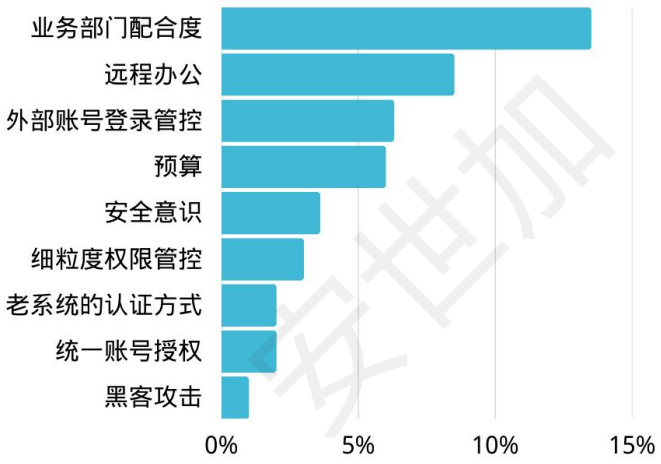


图 24 安全规划挑战

3.3 新一代身份认证管理能力特点

- **企业数字身份统一认证管理**

全域统一管理、公有云和本地数据中心统一管理。打破原有系统间的认证管理隔阂，使用一套更智能的企业身份认证管理系统连接“设备、应用和系统”的全数字化场景，还包括企业内部会议室、数据中心、打印机、梯控等办公物理空间的身份统一管理。

- **安全要求更高**

从“账号管理”提升到”人员管理”的全面管理。身份被盗取的主要原因是密码问题，让员工使用基于 AI 生物特征识别技术的身份认证管理系统，形成基于“人员”的企业数字身份，实现全流程可追溯的身份管理。

- **智能要求更高**

利用更安全的生物识别能力打造兼顾便利性和安全性的全域身份认证能力。静态密码属于“我知道”，多因素认证属于“我知道+我有”，生物特征识别认证属于“我是”，这三者是一个递进的关系，也是企业在落地身份认证管理所追求的“证明我是我”的手段。AI 算法赋能的多因素认证，高精度人脸比对+防伪鉴活技术，可应对伪造欺诈、确保身份可信。

- **效率要求更高**

开箱即用和更全面的兼容性，降低安全和 IT 的管理成本。能在原有身份认证管理体系中直接升级其能力将是首选，尽可能地减少二次开发投入是企业追求快速落地的要求；建设完成后的低成本管理也是降低企业 IT 管理成本的内需；低风险登录场景下，员工可以免密登录个人电脑、云端应用、邮箱、SSO 等，减少对密码的依赖，实现安全与便捷平衡。

- **成本控制更难**

传统基于短信的 MFA 具有一定的成本，当业务系统数量增加后，相应的身份认证管理成本也会同步增加，一次针对短信接口的攻击可能会造成巨大的经济损失。降低 MFA 所产生的

附加费用也是企业重点考虑的因素。

第四章

智能企业身份认证管理场景

四、智能企业身份认证管理场景

4.1 场景一：78%的受访企业高管希望 IT 能提供更全面安全的员工身份管理能力

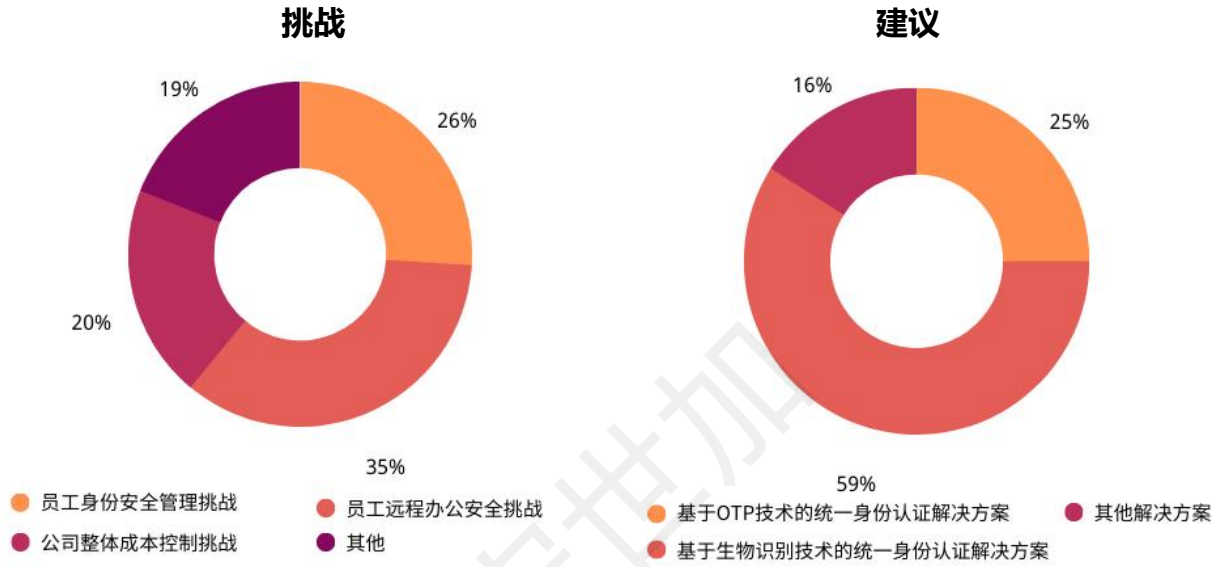


图 25 员工身份管理挑战与建议

企业高管普遍认为统一身份认证管理能力非常重要，特别是对于人脸识别技术的生物识别技术的全面应用抱有很高的预期，另一方面他们也担心成本因素会在一定程度上成为阻碍其全面推进基于人脸识别等生物识别技术为主的统一身份认证体系的落地。

推荐的应对策略：

- 针对关键部门或人员，采用双因素认证方式等牢固 Windows、Mac，及信创等操作系统；
- 可使用人脸认证方案作为第二因素进行认证，如旷视 FaceID 企业版智能身份管理方案，不仅能够提供双因素认证方案登录操作系统，还可针对低风险的登录场景，仅使用刷脸进行免密认证，实现安全与便捷的平衡。

4.2 场景二：92%的受访企业高管觉得需要更有效的手段去管理企业内部 IT 人员

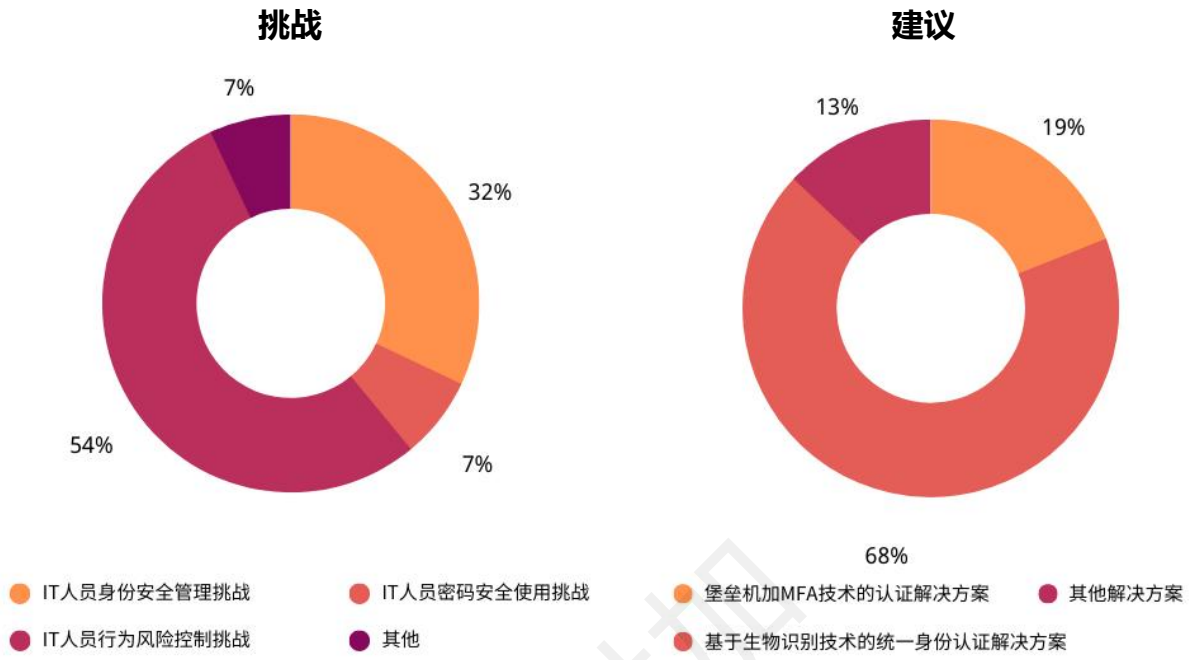


图 26 IT 人员身份管理挑战与建议

近些年由于企业内部技术人员造成的企业损失案例频发，这也增加了企业高管对于内部 IT 人员的管理要求。现有堡垒机加 MFA 的技术方案在很大程度上能够防止内部 IT 人员的“删库跑路”行为，但企业高管更希望能够通过全面审计和全面管控的方式来杜绝类似恶性事件的再次发生，人脸识别为基础的统一身份认证解决方案成为了他们的不二之选，来自法务部门的关于证据留存和审计部门的审计要求也促使企业内部管理层下决心去落实该方案。

推荐的应对策略：

- 启用密码+生物识别技术的 MFA，如旷视 FaceID 企业版可在不改变服务器现有账号体系的情况下，实现共享账号、特权账号的登录管理。这与目前仅针对应用层面身份认证的 OTP 方案相比，其最大优势就在于它能够进行操作系统层面的认证管理，包括 Windows、

Linux 以及信创等系统。

- 生物特征将“账号行为”强绑定至“员工行为”，高风险登录行为精准追溯至个人。

4.3 场景三：83%的受访企业高管希望在企业内提供无密码化的办公体验

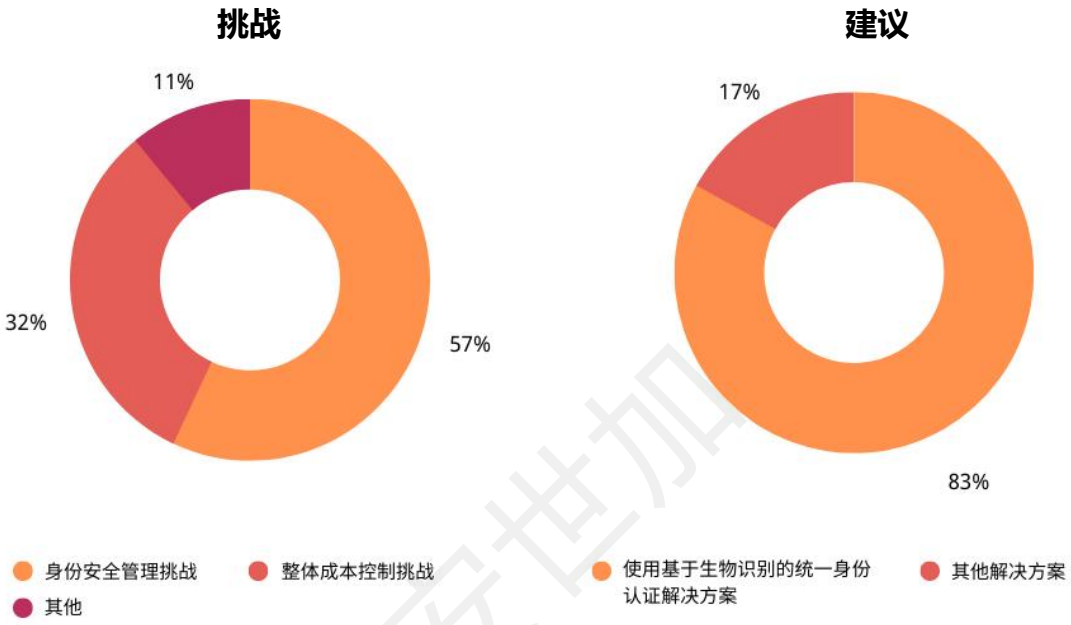


图 27 身份管理挑战与建议

在受访的企业中，高管和员工对于无密码化的数字化环境都保持了相同的积极接受态度，这也侧面体现出近些年随着企业信息安全建设所带来的一个侧面影响，密码太多太复杂了，其中固然有未有效落地统一身份管理的因素，但也的确反映了安全与用户体验之间的平衡难度。随着以人脸识别为代表的生物识别技术的成熟，这一平衡很有可能将得到质的飞跃，部分企业高管甚至已经在全力推动基于人脸识别技术的统一身份认证系统的改造了。

推荐的应对策略：

旷视 FaceID 企业版免密登录方案，平衡用户体验和安全。

第五章

研究案例

五、研究案例

5.1 案例背景

我们有幸获得部分企业的授权和大家分享他们在做企业身份认证管理工作中的真实案例，本案例将以一家虚拟的企业 Z Company 为背景展开，Z Company 是一家发展迅速的快消赛道的企业，他们在全国各地拥有众多的经营网点，最近正考虑发展海外业务，目前员工数量已经超过 10000 人。公司 CIO Peter 正在为如何满足高速发展的业务需求和提升用户使用体验而焦虑，经过多轮沟通和规划，他决定从身份认证管理入手，构建企业统一的身份认证管理能力，逐步提升用户体验和安全性，逐步将所有业务系统接入，实现公司整体数字化能力的提升。

5.2 设计新一代身份管理认证体系

Peter 和团队以企业实际业务为出发点，在梳理了现有信息化系统和业务部门的痛点后，明确了第一步需要完成的工作，明确新一代身份管理系统的基本需求，简单概括为以下几点：

- 以确保业务流程高效、安全、稳定运行为基础；
- 统一的标识管理，即一个 ID 覆盖所有公司数字化场景；企业数字统建和物理空间的统一管理，即贯穿所有的应用、系统和设备，有足够的灵活和兼容性；
- 共享账号、公共账号的实名管理，即每次共享账号登录时，确认操作者身份；
- 增强可审计性，即有能力提供充分有效的运行评估报告，运维事故发生时能够锁定到具体人员；

- 优秀的用户体验，即员工使用基本无感，90%的场景用户可以不需要记录密码；
- 自适应的安全访问控制，基于安全风险和应用场景的自动识别和调整，既不影响用户使用又能够做到权限有效的动态调整管控。

下一步，Peter 和团队需要将这些需求细化，形成能够落地的整体解决方案。首先就是他们需要选择什么样的身份认证平台，其次分别是面向企业业务部门和 C 端、B 端、E 端的需求细化和调整。在本案例中，Peter 决定采用基于 Active Directory 为基础的核心目录服务和人脸识别技术相结合的整体技术方案，其主要考量是久经考验的 Active Directory 具有非常稳定的可靠性和可扩展性，其次就是人脸识别技术给用户所带来的极致体验和更为可靠的安全性。

图 28 基于人脸识别技术的新一代身份认证管理体系，以“人”为核心，从数字空间到物理空间的多元化管理

5.3 落地新一代身份管理认证体系

在项目落地的过程中，Peter 和团队在具体的落地细节中明确了以下需要特别注意的事项，因为这些事项的落地程度将决定整个方案的后续效果，大致归为以下部分：

- 使用单个 Active Directory 实例，主要是考虑点是保持其一致性和权威性，降低错误配置和可能的同步问题影响其可靠性；
- 账号分级分类管理，将高权限的管理账号和普通账号区分管理；
- 使用单一登录 SSO，为了提升用户的体验，最大程度上降低用户需要主动使用密码的场景和次数；
- 使用自适应访问策略，这部分能力借助于我们的合作伙伴提供的安全和动态策略控制能力，最大程度上降低了 IT 人员的维护成本；
- 最小授权策略，即权限够用即可，能以低权限运行的绝不授予高权限；
- 使用 MFA，在特定的业务场景中明确要求用户启用 MFA，这已经被印证是更为有效的安全手段；
- 保留账号自助注册能力，在部分 B 端和 E 端场景中为合作伙伴和员工提供该能力将有效的提升业务部门的活力；
- 保留第三方身份验证能力，在与不同客户的商务活动中允许将数据与第三方系统联系以实现业务互通，是保持和一些战略伙伴密切合作的一种高效手段；
- 持续的优化和迭代，以有效和稳定为基础的优化系统。

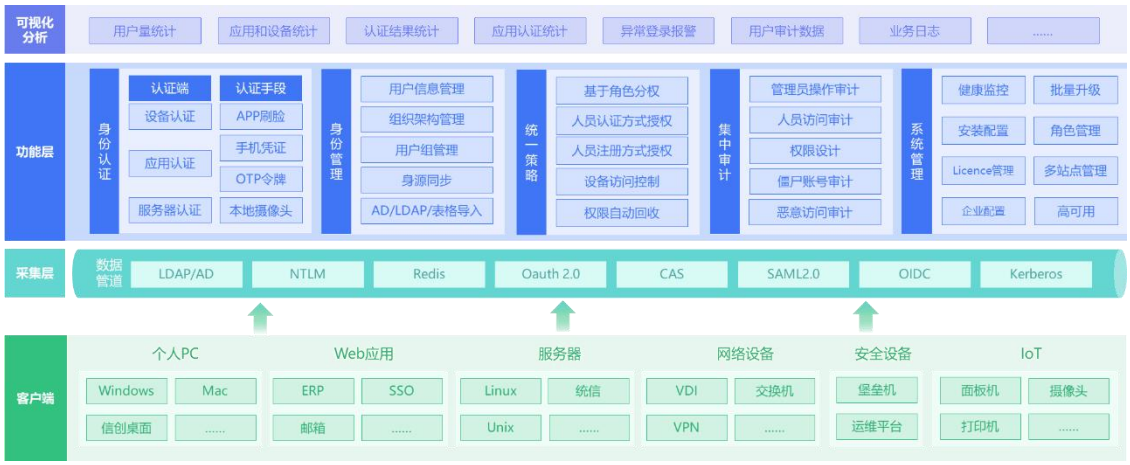


图 29 新一代身份管理认证体系图

5.4 生物识别技术的应用

Peter 和团队将系统设计成可以同时使用密码或人脸识别的状态，主要是考虑到部分人员可能对于生物识别技术的使用存在疑虑，不能一刀切的粗暴全部使用生物识别技术。有趣的是在经过一段时间运行后，人脸识别技术的使用率明显高于密码的使用频率，在年度系统调研中，绝大部分反馈是对于生物识别技术便利性和安全性的认可，当然这也少不了 Peter 和团队在日常工作中对于信息安全工作的重视，不定期的开展安全开放日工作、定期的外部信息安全审计和安全认证等等工作，都是对于公司和员工的一种保护。

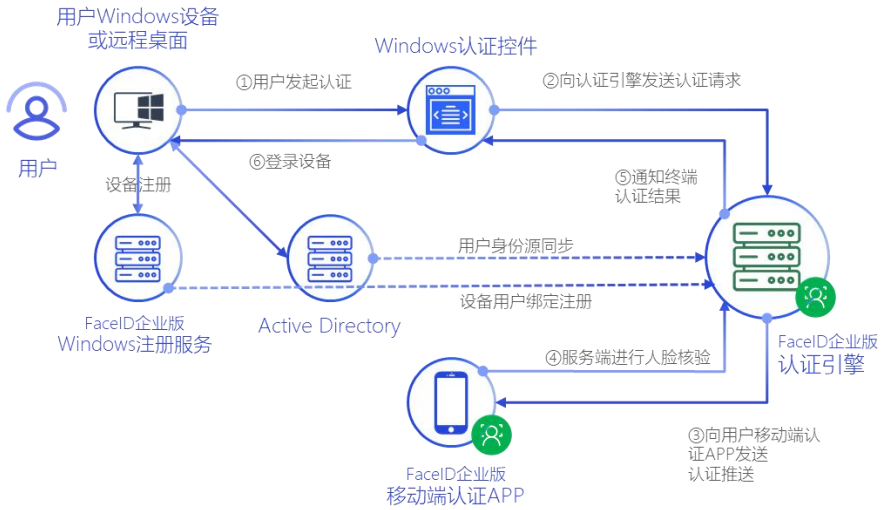


图 30 企业员工身份认证场景举例-Windows 设备登录

以上案例是一个简略的新一代身份认证管理体系落地的一个大致过程，其主要核心对于企业真是业务需求的满足，整个身份认证管理项目的落地只用了不到 3 个月，Peter 和他的团队正在努力将散落各地的不同业务系统逐步纳入其新一代身份认证管理体系，这一步很艰难，但今天每一小步的累计，都将为其整体数字化平台能力构建打下扎实的基础。

第六章

安全建议

六、安全建议

绝大部分企业都有他们的身份认证管理解决之道，很大一部分是基于 AD 作为技术实现的，对于部分已经能够满足企业需求的情况，建议这部分企业可以不必操之过急，有效的运营好你的身份认证管理能力才是重中之重。对于有建设需求的企业，可以参考我们的如下建议：

在安全技术方面，我们需要重点关注：

- 有效的账号管理，永远不要否认企业存在应该删除、禁用，但却仍然可用的账号；
- 根据企业实情，有顺序有计划的落地身份认证管理能力，不要想着一步到位；
- 在设计身份认证管理架构体系时，充分考虑灵活性、混合云、多云环境；
- 尽早地落实基于生物识别技术的身份认证管理能力，大量实践已经充分说明了它能有效平衡便利性和安全性。

在组织能力方面，我们需要重点关注：

- 业务部门的真实诉求是什么，很多时候需求的变更源于真实诉求的误解；
- 业务部门必须是身份认证管理项目组成员之一；
- 技术部门必须懂得业务语言，能够用非技术语言和业务部门沟通。

调研方法

我们的访谈时间为 2022 年 6 月至 2022 年 12 月期间，我们对超过 100 家组织的主要安全负责人进行了单独访谈，收集了大量深入的真实信息。

为了保护被调研对象的机密性，我们没有获取被调研企业的特定具体数据信息，数据收集主要通过多种访谈的方式开展，不包括实际会计信息等，访谈对象所提供的数据均在样本范围内进行了处理，以确保数据的真实可靠以及对被调研对象的保护。

北京旷视科技有限公司

旷视是一家聚焦物联网场景的人工智能公司。基于业界领先的人工智能基础研究与工程实力，旷视面向消费物联网、城市物联网和供应链物联网三大核心场景提供历经验证的 AIoT 产品和解决方案，持续为客户和社会创造价值。

旷视自主研发了新一代 AI 生产力平台 Brain++，助力 AI 技术实现了从算法生产到应用的全流程化和规模化供给。源于 Brain++强大的 AI 能力，旷视打造出完整的 AIOT 产品体系，包括 AIoT 操作系统、AI 重新定义的硬件、AI 重新定义的行业应用。

旷视 FaceID 企业版是以“人”为核心的企业空间身份管理方案。基于 AI 赋能的生物特征识别技术，打造新一代多因素身份管理平台，实现企业空间内“人员-设备-系统-应用”统一管理，为客户提供更安全、更智能、更高效的办公和生产体验。

旷视成立于 2011 年，旷视拥有全球规模领先的计算机视觉研究院，并在北京、上海、南京、成都等地均设有研发中心。

扫码关注官网微信

支持单位


陌陌安全
苏宁安全应急响应中心
Suning Security Response Center
顺丰安全应急响应中心
SF Security Response Center
合合安全应急响应中心
Intsig Security Response Center
贝壳安全应急响应中心
BOSS直聘安全应急响应中心
中通安全应急响应中心
ZTO Security Response Center
vivo安全应急响应中心
vivo Security Response Center
字节跳动
安全中心
讯飞安全
OPPO 安全应急响应中心
OPPO SECURITY RESPONSE CENTER
快手安全应急响应中心
SECURITY RESPONSE CENTER
瓜子安全应急响应中心
GUAZI Security Response Center
智联招聘安全应急响应中心
Zhaopin Security Response Center
微众银行安全应急响应中心
WeBank Security Response Center
HONOR

支持媒体


IT经理网
CTOCIO.com
Secfree.com
指尖安全
安全脉搏
SECPULSE
CI14
www.CI14.com.cn
东方安全
企业网 D1Net
企业IT第1门户
铁匠运维网
tiejiang.org
ENI cn.com
经济和信息化
嘶吼
ROARTALK
游侠安全网
WWW.YOUXIA.ORG
互联网之家
RadeBit瑞安全
www.radebit.com

支持自媒体


謝公子學安全
暗影安全
shadowsec
GCOW
安全团队
WhITECat
安全团队
TIMELINESEC
一起聊安全
火山信安实验室
蛇矛实验室
SNAKE SPEAR LAB
洞见网安
DOONSEC.COM
寻云安全团队
WgpSec
Sec盾
security shield
V安全
哈拉少安全小队
HLS SAFETY TEAM