



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

安全的最后一公里：特权访问安全



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

数字经济下的特权账号威胁

企业IT发生了哪些变化？



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

企业数字化转型



应用系统变得越来越多
数据变得越来越重要

打通信息孤岛



系统之间的交互变得越来越多

向云的转变



IT环境变得越来越复杂

DevOps生态的建设



DevOps工具变得越来越多



结论：

特权账号数量、种类变得越来越多

特权账号的使用场景越来越复杂

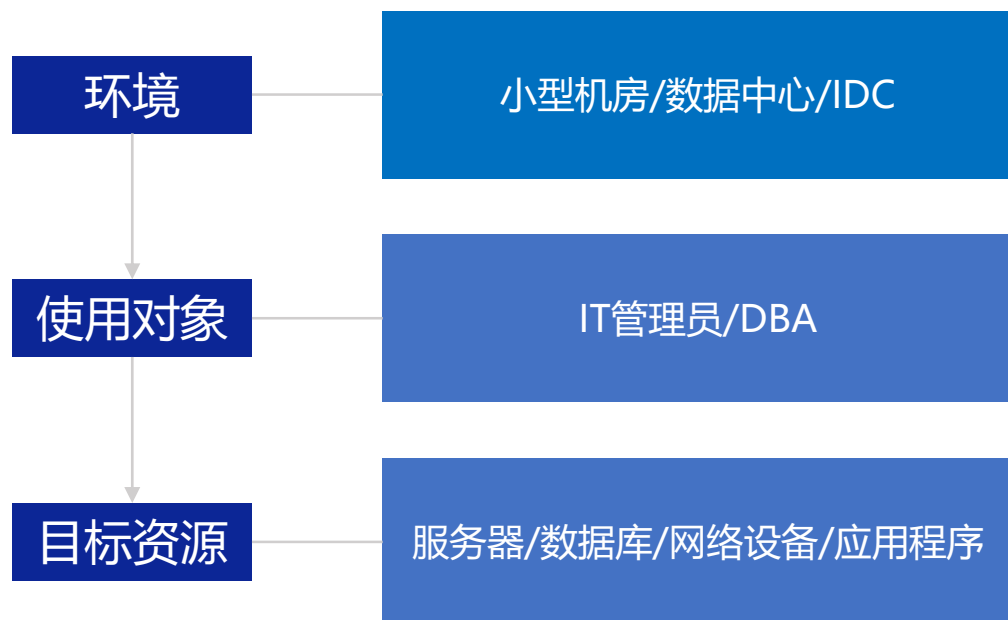
特权账号的安全威胁和管理挑战越来越大

特权账号的使用场景发生了哪些变化？

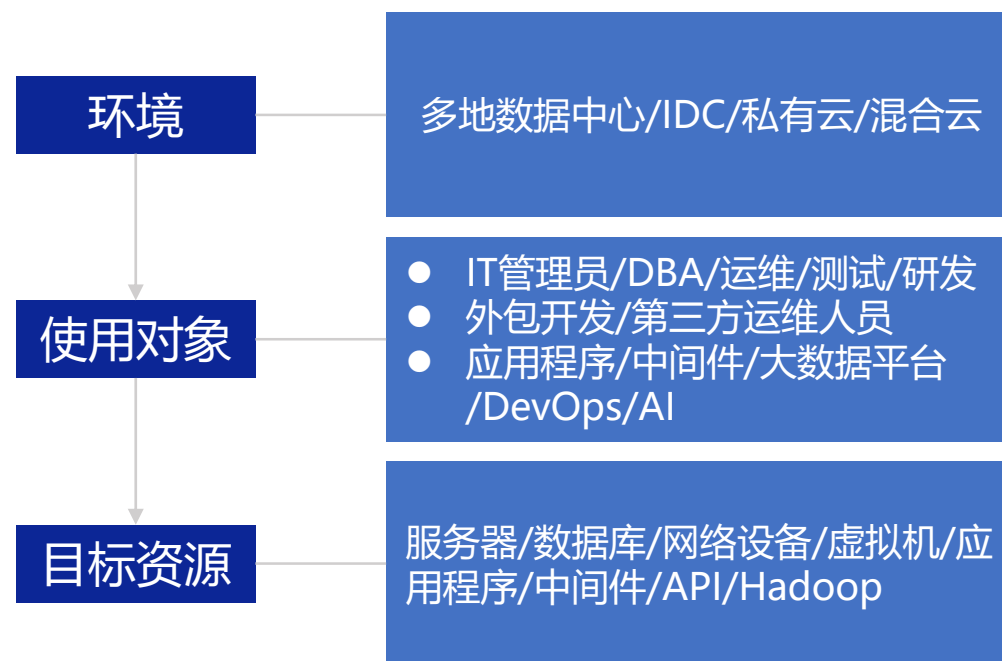


2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

过去



现在



特权账号是数据安全的最后一道防线



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

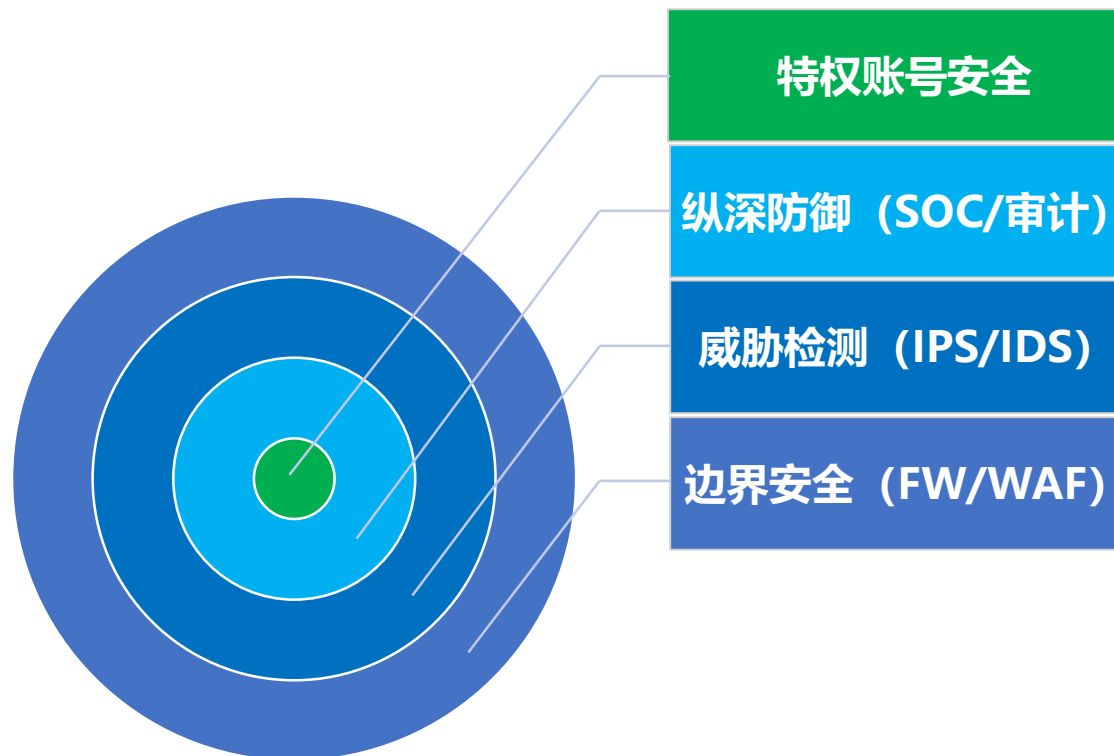
获取特权账号是黑客成功的必要条件！

“100%的信息泄露都涉及到了**凭据丢失**……”

“高级持续性威胁APT首先尽各种可能**找到可以利用的特权账号**，例如：域管理员、具有域权限的服务启动账号、本地管理员账号和拥有业务特权的账号。”

——Mandiant, M-Trends and APT1 Report

安全边界 →
威胁检测 →
纵深防御 →
核心数据 →
层层突破 →



行业趋势—PAM成为最重要的安全领域之一



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

	2014年	2016年	2017年	2018年	2019年
IAM	自适应访问控制			特权访问管理PAM	特权访问管理PAM
	软件定义的安全SDS		软件定义边界SDP	软件定义边界SDP	



安全运营	是下一代安全平台的核心	核心及编排解决方案技术	可管理检测与响应MDR	检测与响应之MDR	符合CARTA的弱点管理	符合CARTA的弱点管理 安全事件响应平台 安全评级服务
------	-------------	-------------	-------------	-----------	--------------	------------------------------------

Gartner历年评选的顶级技术/项目对比分析



- 各类主机操作系统的管理账号，如AIX、WINDOWS、LINUX.....
- 各类数据库系统的管理账号，如ORACLE、SQLSERVER、DB2.....
- 各类中间件系统管理账号，如WEBSHPERE、WEBLOGIC、TOMCAT（连接池账号、Web Console）.....
- 各种设备的管理账号，如路由器、交换机、VPN、工业设备.....
- 各种安全系统和设备管理账号，如防火墙、入侵检测、防病毒.....
- 应用系统内嵌账号，如应用系统源码、配置文件、中间件中的数据库访问账号、API接口账号、Web Console.....
- 业务前台管理账号，如核心业务系统前台的管理账号、批量数据下载账号、用户管理账号.....

什么是特权账号？

特权账号管理面临哪些挑战？



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

技术挑战

可视性不佳

很难看到存在什么账户，
谁在使用这些账户

难以有效管理

很难保障账号密码的安全

缺乏控制手段

请无法看到谁在用哪个帐号
在做什么，没法控制特权账
户的权限

业务风险

数据泄露的风险

特权账号使用静态密码，对账户缺乏管
理、监控方法，企业容易遭受攻击

审计失败与合规风险

很多法规要求企业管理特权账号密码并监
控特权账户使用

如何应对这些挑战？



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

解决方案

账号自动发现

自动发现并纳管特权账号，
实时跟踪特权账号的变化

全生命周期管理

自动创建、修改、删除特权
账户的密码

控制与监控

通过视频、日志两种方式同
时记录会话；监测特权账户
使用异常情况

业务收益

降低安全风险

保障和控制特权账号远离威胁；实时监
控会话及登录分析功能能够实时发现
正在进行的黑客攻击

合规

遵从针对特权账户安全的法律法规，如等
保2.0、金融服务信息安全指南、银监会令
2007年第6号、银监发「2016」44号等



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

建设方案与产品能力

特权账号安全该怎么建设？



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

账号发现与梳理

- 1) 各系统里都有哪些特权账号？
- 2) 谁拥有这些特权账号的访问权限？
(包含人和机器)



建立规则

- 1) 按照业务所需建立授权访问规则（组与策略）；
- 2) 对特权账号密码的安全存储、使用及定期轮换规则的建立。



建立标准

新系统建设，都需要通过既定标准进行特权账号的申请和使用。



监控与分析

对特权访问的行为进行监控与分析，发现潜在威胁并及时阻断。



账号发现

- 发现账号列表
- 收集账号基础信息，权限信息：

自动改密

- 实现各类账号的自动密码修改、验证、重置
- 丰富的密码策略，适配各类设备
- 密码引用处的同步更新

安全存储

- 独立安全存储
- 国密加密保护
- 硬件加密

账号策略

- 统一入口管理账号的增删、权限编辑、解锁/锁定，无需管理员登陆系统
- 密码备份、历史密码、分段管理

应用访问控制

- 应用访问各类账号资源
- 内部关联系统获取账号资源

风险管理

- 评估各个业务系统的账号合规情况
- 发现弱密码、僵尸账号、幽灵账号
- 权限变化过程
- 账号巡检

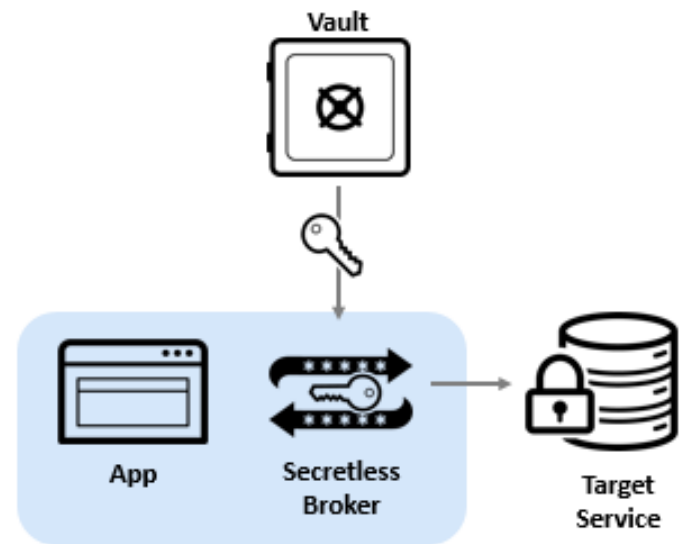
最佳实践一：消除“硬编码”



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

应用、服务、脚本等内嵌大量特权账号，在与系统、数据库、云对接交互过程中潜藏着巨大的安全风险！

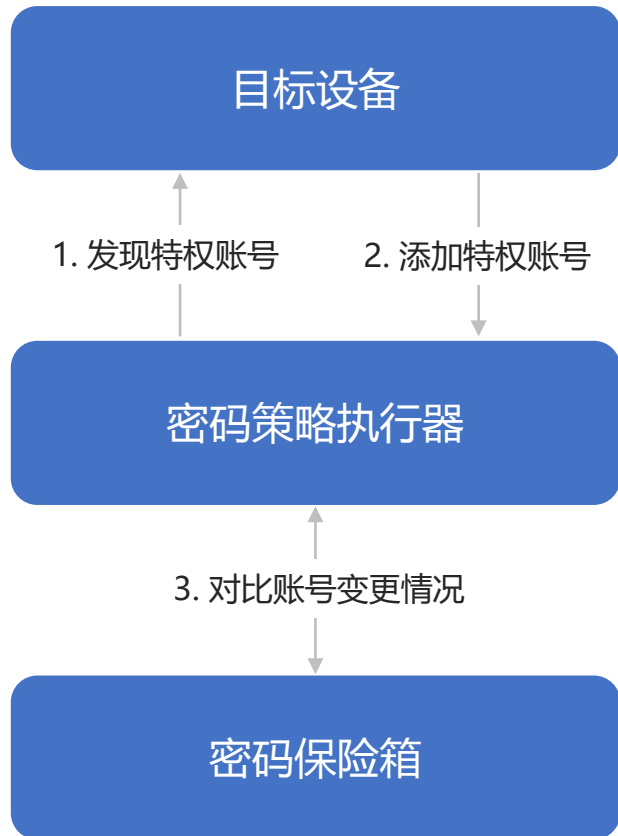
1. 避免在应用、服务、脚本内“写死”密码，使用更安全的数字保险库技术加固此类特权账号，使用“API身份”认证技术获取“最新”的密码。
2. 此类密码由于不能实施“多因素”技术，应使用数字保险库技术定期改密，对于密码、密钥的调用、使用要有详尽的审计，审计日志要做到不可篡改。
3. 确保定期改密对关键应用“零”影响，例如不能中断业务、自动化流程等。
4. 关键业务应用、业务容器在调用密码、密钥时，要进行强认证确保其“身份”，防止“非法”应用冒用密码、密钥。
5. 确保业务容器大规模并发访问时，密码、密钥的高可用和高效性。



最佳实践二：特权账号自动发现与追踪



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE



- 管理员通过账号发现功能，可自动发现企业内部Linux系统和AD域的特权账号，简化特权账号的录入操作。
- 管理员可以设置定期扫描账号分布情况，及时发现未纳管的特权账号。
- 通过对比历史的账号发现日志，分析特权账号的新增、删除、权限修改等情况，及时发现可疑账号。



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

THANKS

全球网络安全 倾听北京声音