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

内生安全 从安全框架开始

ENDOGENOUS SECURITY:
STARTING FROM A CYBERSECURITY FRAMEWORK

安全的最后一公里：特权访问安全

嘉宾照片

嘉宾

王爱兵

奇安信-哈工大（深圳）数据安全研究院
副院长

数字经济下的特权账号威胁

企业IT发生了哪些变化？

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

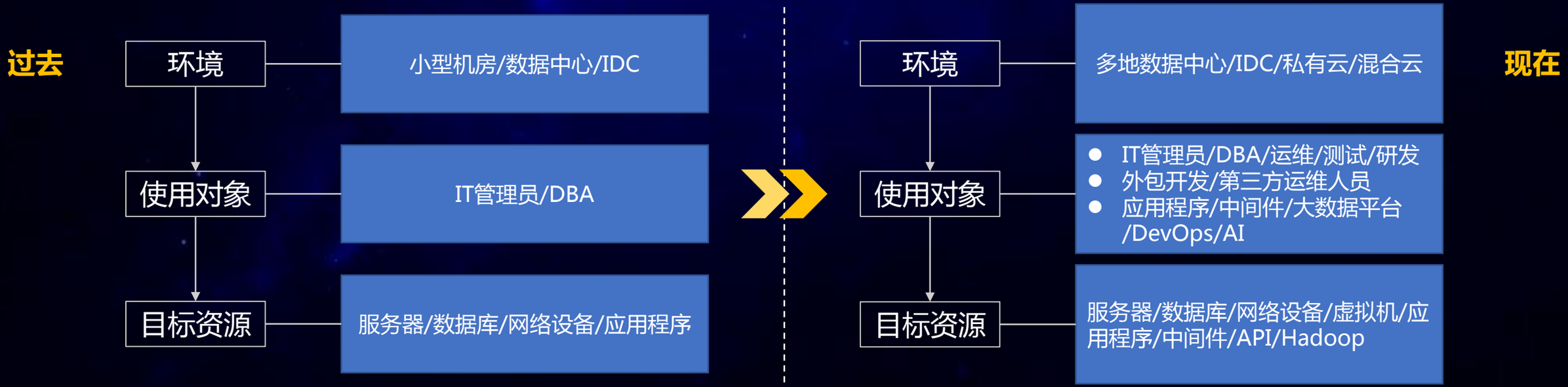
结论：

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？



特权账号是数据安全的最后一道防线

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

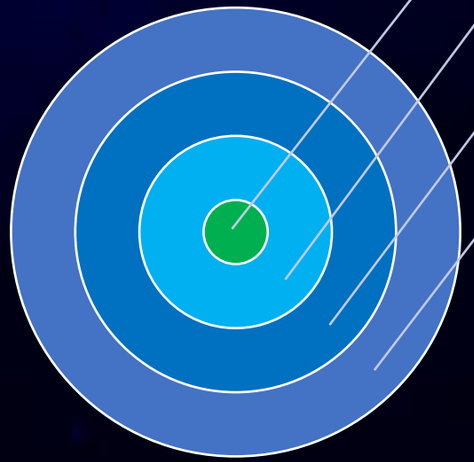
安全边界 →

威胁检测 →

纵深防御 →

核心数据 →

层层突破 →



特权账号安全

纵深防御（SOC/审计）

威胁检测（IPS/IDS）

边界安全（FW/WAF）

行业趋势—PAM成为最重要的安全领域之一

	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
云安全	软件定义的安全SDS		软件定义边界SDP	软件定义边界SDP	
	云访问安全代理CASB	云访问安全代理CASB	云访问安全代理CASB	云访问安全代理CASB	云访问安全代理CASB
		微隔离	微隔离	微隔离	
			云工作负载保护平台CWPP		
				云安全配置管理CSPM	云安全配置管理CSPM
端点安全	端点检测与响应EDR	端点检测与响应EDR	端点检测与响应EDR	检测与响应之EDR	检测与响应之EDR
		基于非签名方法的端点防御技术			
				服务器工作负载的应用控制	
网络安全	遏制与隔离将作为基础的安全策略	远程浏览器	远程浏览器		
		欺骗技术	欺骗技术	检测与响应之欺骗技术	
			网络流量分析NTA		
	机器可识别的威胁情报（包括信誉服务）				
	沙箱普遍化				
		用户和实体行为分析UEBA		检测与响应之UEBA	
				积极反钓鱼	商业邮件失陷
应用安全	交互式应用安全测试	DevOps的安全测试技术	面向DevSecOps的开源软件安全扫描与软件成分分析	自动安全扫描:面向DevSecOps的开源软件成份分析	
			容器安全		容器安全
数据安全					暗数据发现
IoT	针对物联网的安全网关、代理和防火墙	普适信任服务			
安全运营	大数据安全分析技术是下一代安全平台的核心	情报驱动的安全运营中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

Gartner 分析师认为**任何组织**都需要解决特权账号以及其他拥有高级权限账号的安全问题，因为这些账号一直是攻击者的**首要目标**，利用这些账号可以**轻易获取敏感信息和数据**。

- 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？

技术挑战

可视性不佳	难以有效管理	缺乏控制手段
很难看到存在什么账户，谁在使用这些账户	很难保障账号密码的安全	无法看到谁在用哪个帐号在做什么，无法控制特权账户的权限

业务风险

数据泄露的风险	审计失败与合规性风险
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	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？

解决方案

账号自动发现	全生命周期管理	控制与监控
自动发现并纳管特权账号，实时跟踪特权账号的变化	自动创建、修改、删除特权账户的密码	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	合规
保障和控制特权账号远离威胁; 实时监控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	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

建设方案与产品能力

特权账号安全该怎么建设？

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。

特权账号治理实践思想

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

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

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

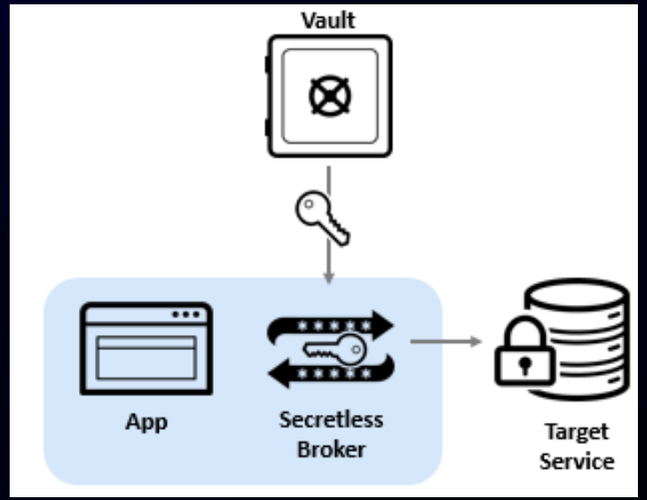
账号发现
- 发现账号列表
- 收集账号基础信息，权限信息：

风险分管理
- 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

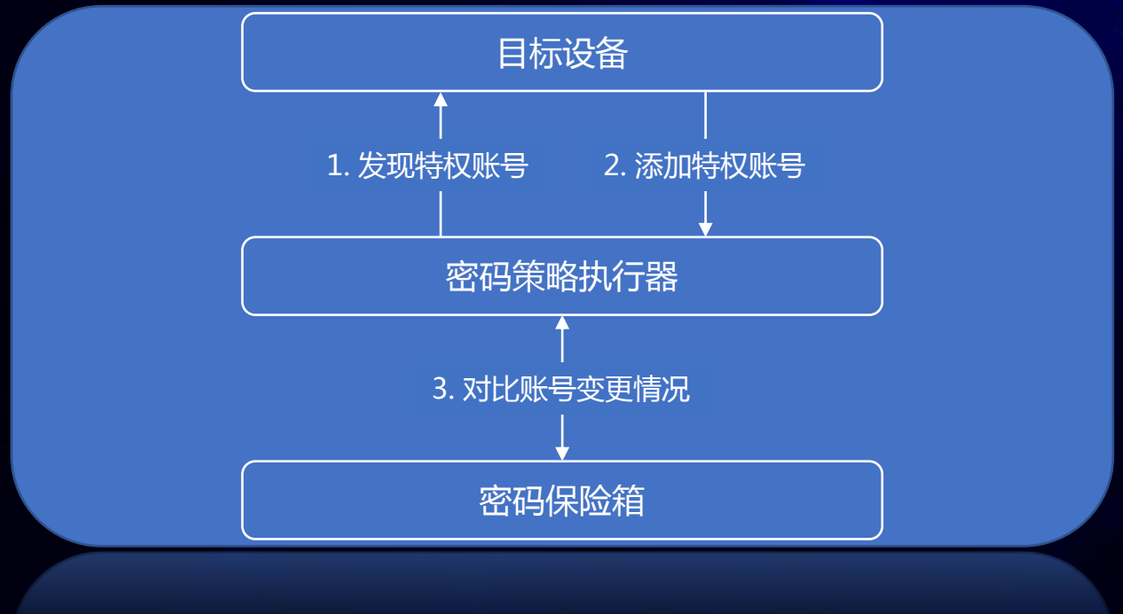
最佳实践一：消除”硬编码“

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



- 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。

谢谢！