



数字银行零信任网络实践

网商银行 张欧

# 目录

## CONTENTS

01. 挑战
02. 零信任网络实践中的误区
03. 从零信任到可信网络
04. 策略运营与部署的原则

# 从钓鱼邮件开始

**Your Invoice is available. Please remit payment at your earliest convenience.**

**Account Number: U7133660**

**Invoice Number**

397594

**Amount**

1,455.18

Click below to connect eInvoice  
System

亲!

您**2011-2019**历年的健康报告已同步更新。

您可以登录 [我的健康](#) 查看健康指数曲线和健康指导建议。

如果您的健康报告中存在需要改善的部分，请您务必重视。如果您对健康报告中的指标有疑惑，或者想要更加深入地了解自己的健康报告，欢迎拨打健康平台上方的报告解读热线，为您的健康保驾护航！

此邮件为系统邮件，无需回复。如有问题，请联系健康中心热线， 谢谢！

Dear,

Please see attached Invoice dated 09/26/2018.

Thank you,

只要模仿得像，一定会有员工中招

人性的漏洞难以修复

## 认知偏差

0Day漏洞和APT攻击不可避免  $\Rightarrow$  必须做检测和响应  $\Rightarrow$  事前防护被忽视  
纵深检测  $\neq$  纵深防御

## 做好检测和响应够吗

内网是办公/测试/生产几张大网，进入内网畅通无阻

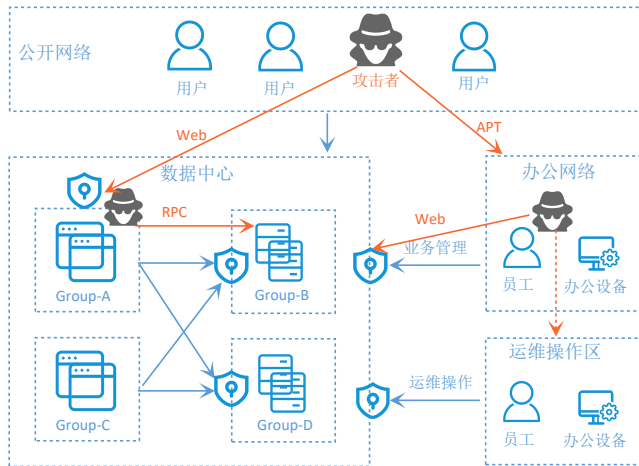
APT、0Day漏洞攻击场景可能来不及响应

事前纵深防护没做好，导致检测和响应的误报增加

风险发生时损失已经形成，资金损失风险高



# 银行场景的网络层纵深防护



不足之处:

应用层访问允许打通, 攻击仍然可以穿透

灵活度底导致低效

网络隔离策略维护成本高

# 新思路

## Zero Trust

- 不信任网络位置
- 最小化访问权限
- 分析和记录所有网络访问流量

## SDP

- 提供软件定义的边界
- 只有通过设备认证和身份认证才能获得访问权限

## 微隔离

- 控制网络内的东西向访问
- 不仅基于IP和端口控制
- 基于流量内容

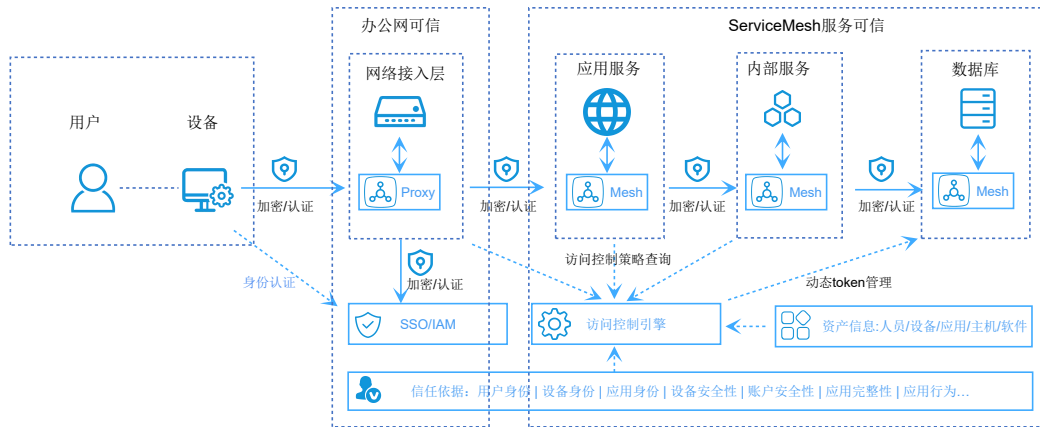
## 零信任网络实践中的误区

BeyondCorp? 解决企业办公系统访问风险?

解决员工身份认证的问题? 和SSO/鉴权有啥区别?

零信任网络是不是什么都不信任?

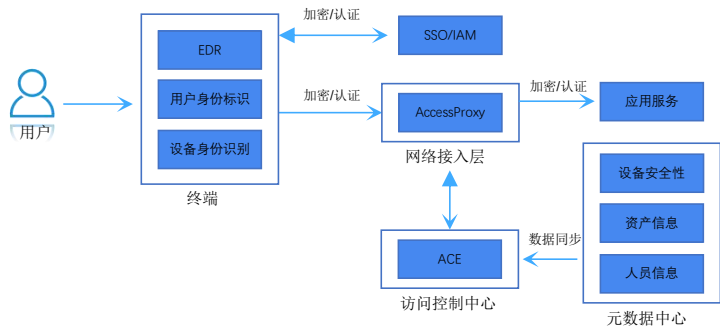
# 从零信任网络到可信网络



从「办公系统网络」到「所有网络行为」

从「允许通过身份认证/鉴权的网络访问」到「仅允许符合预期的网络访问」

# 办公网络可信访问



默认覆盖

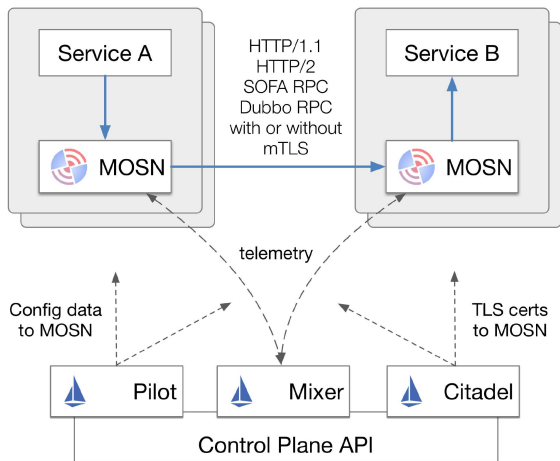
人员认证/鉴权

设备认证

设备安全性

行为合理性分析

## ServiceMesh服务可信



认证/鉴权/访问行为检测

跨平台/多协议/无侵入

高性能/稳定性/可扩展

基于SOFAMesh/SOFAMosn实现

# 策略运营与部署



谢谢

Thanks



张欧 网商银行

参考: Istio <https://istio.io/>

SOFAMosn <https://github.com/sofastack/sofa-mosn>