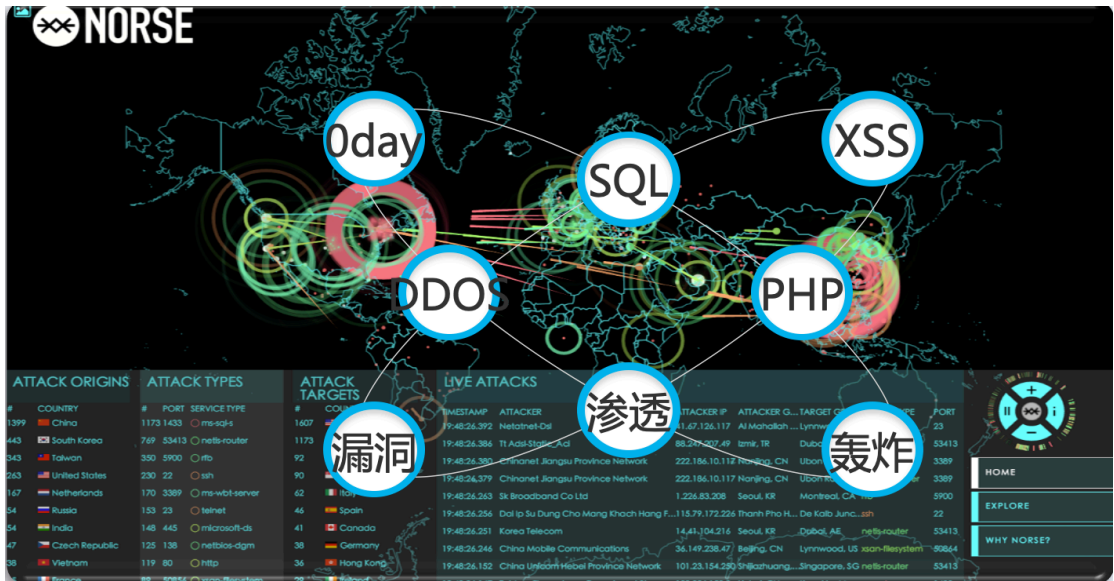


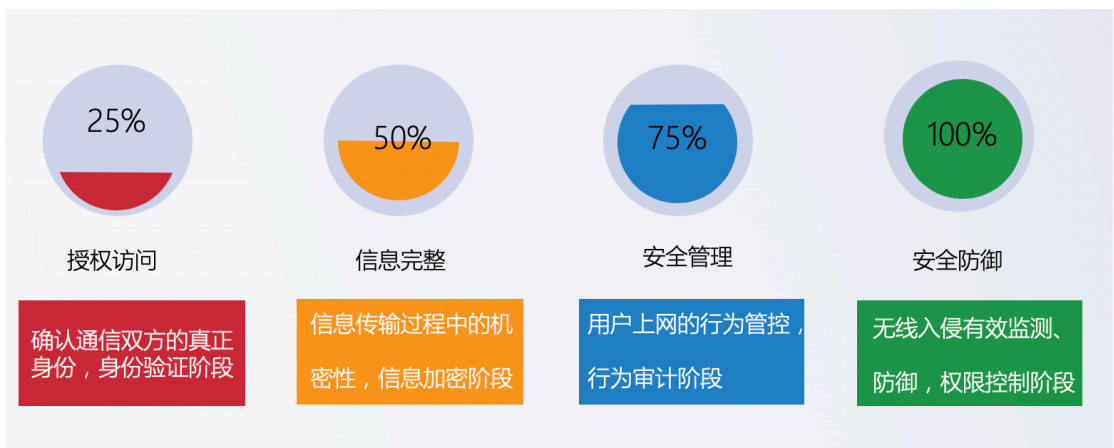
# 无线网络网络安全合规

现如今，安全早已不在是出口的安全问题，贯穿全周期，全业务系统的安全要求。但与有线网络比较，无线安全风险更易发生。



通过无线嗅探、破解工具，非常容易入侵 WEP/WPA/WPA2 加密的无线网络、内网私接 Wi-Fi 泄密，可直接导致非法无线入侵，威胁数据安全、虚假钓鱼 Wi-Fi、无线欺骗、DOS 攻击央视 315 晚会近几年曝光，安全威胁越来越严重。

实现无线网络安全，信锐能做哪些呢？



## 1、无线安全认证及准入

信锐技术将结合终端类型、内外部认证、认证方式等不同维度进行鉴别。比如：基于不同的系统识别终端类型，实现准入策略，哪些网络哪些类型的终端可以接入，接入之后被分配到不同的 VLAN 实现内外网逻辑隔离，匹配不同的认证方式来对身份和权限进行区分。



## 2、上网行为管控

管理员可以基于用户角色、时间计划、AP 位置信息等管控用户上网权限行为，并将其内容进行审计，满足相关法规的要求。



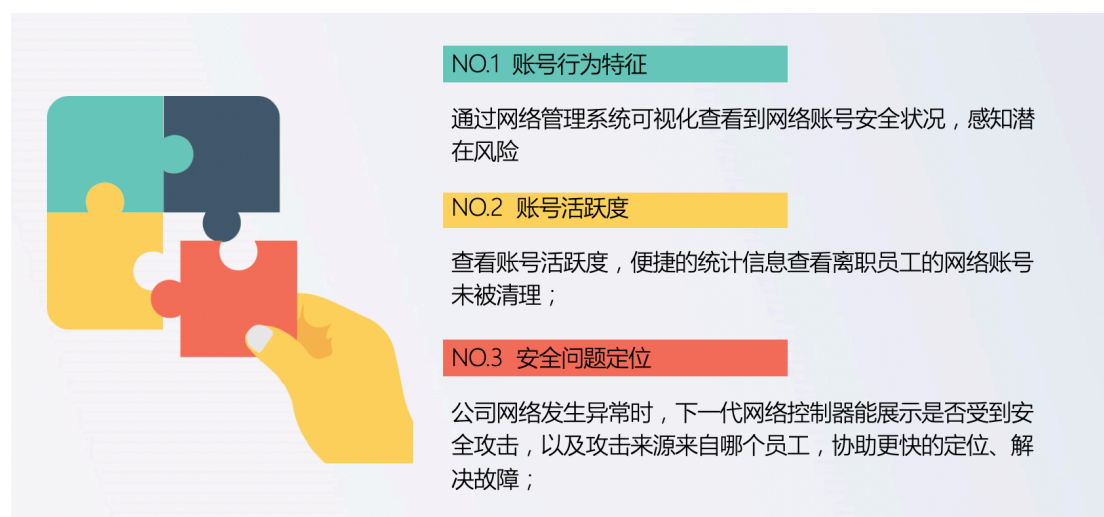
### 3、无线网络东西向流量安全

在正常健康的网络中,终端之间互访的流量一般非常少。当终端与终端之间发生流量时,并且匹配事先配置的规则, 当有异常访问触发规则时则进行相对应的动作。



### 4、账号的安全画像

可视化查看到网络账号安全状况,感知潜在风险,可协助管理员更快的定位、解决故障;



构建端到端的无线安全应用网络,从上网认证前的认证&加密、上网过程中的访问控制策略、以及上网后产生的行为记录。以及日常维护防范所需要的攻击检测与防御,账号安全状况等。



## 01

### 上网前：认证&加密

- 802.1X, Web, 移动OA, MAC, 短信认证, 微信小程序认证, 二维码认证、智能PSK...
- 802.11i, WPA / WPA2...
- TKIP, AES, CCMP

## 02

### 上网中：集成策略防火墙

- 基于全国领先的应用规则库的应用控制
- 基于用户、用户组、终端类型、接入位置、时间段的控制策略

## 03

### 上网后：上网行为记录

- 审计记录所有用户上网行为, 包括访问的网站、收发的邮件、论坛微博发帖等, 满足公安部82号令

## 04

### 无线防御：入侵检测/攻击防护

- WIDS/WIPS、防DoS攻击
- 防欺骗攻击、防泛洪攻击、内网东西向流量...
- 动态黑名单

## 05

### 安全大数据分析：账号安全画像

- 可视化查看网络账号安全状况, 查看账号活跃度
- 针对无线终端的边缘防护, 防止中毒终端非法扫描内网其他合法终端。