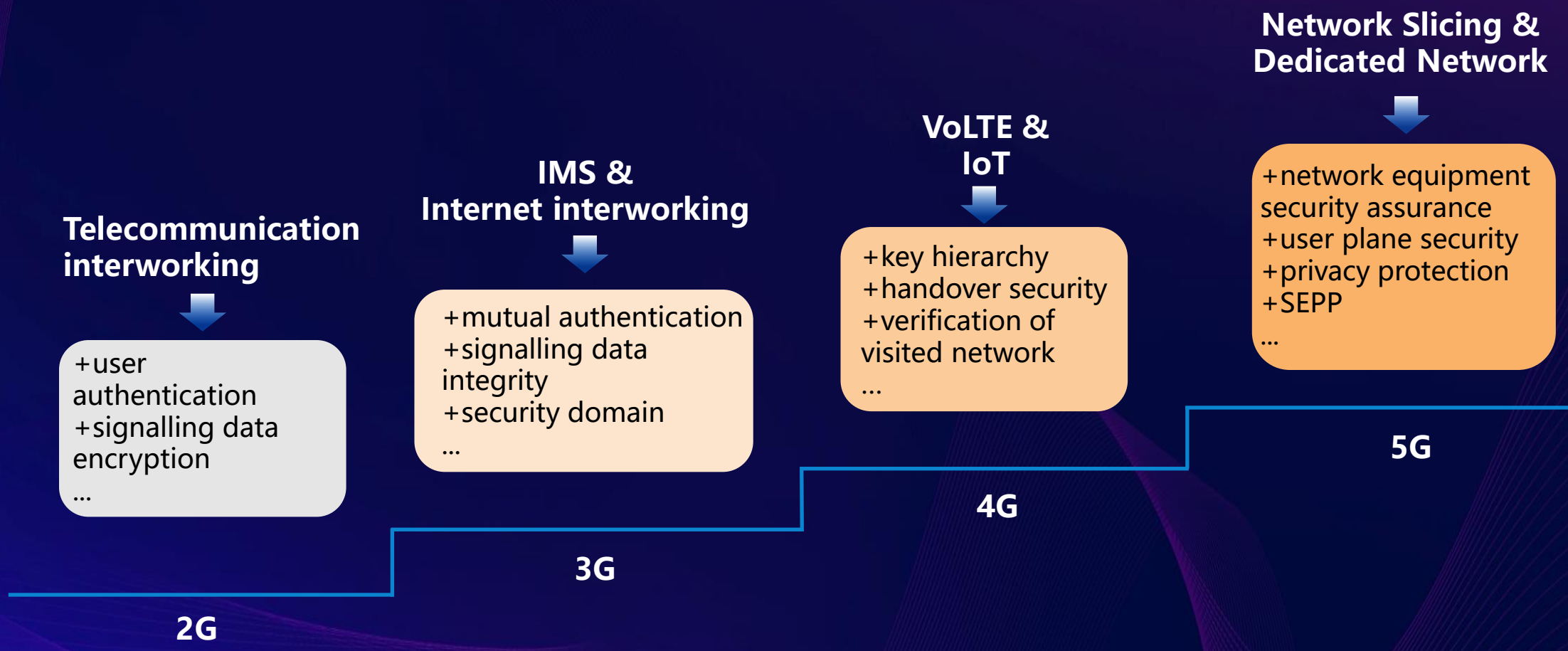
Fine-Granularity Segmentation Solution for 5G Network

China Mobile

2024.11

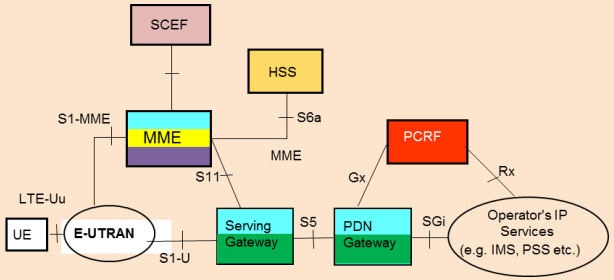
2G-5G: Continuously Enhanced Security



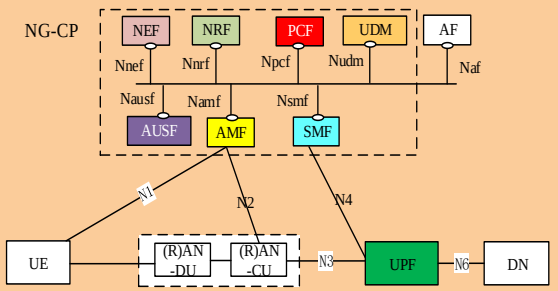
Different level of decoupling brings increasing internal attack path

- 4G: Decoupled hardware and software enables internal attacks
- 5G: Decoupling of hardware, virtualization and software increases the internal risk
- 6G: interactive invocation between services; Multi-dimensional capability services are decoupled from network elements and resources

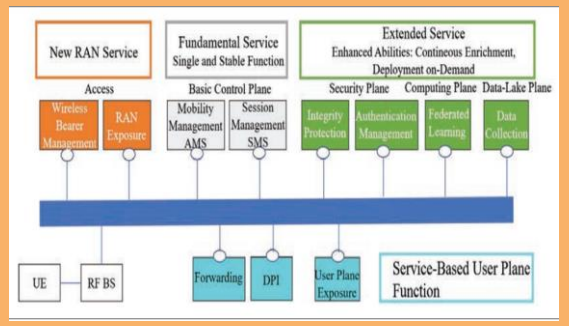
4G



5G



6G



Hardware and software decoupled deployment → **Service decoupling** → **Capability decoupling**

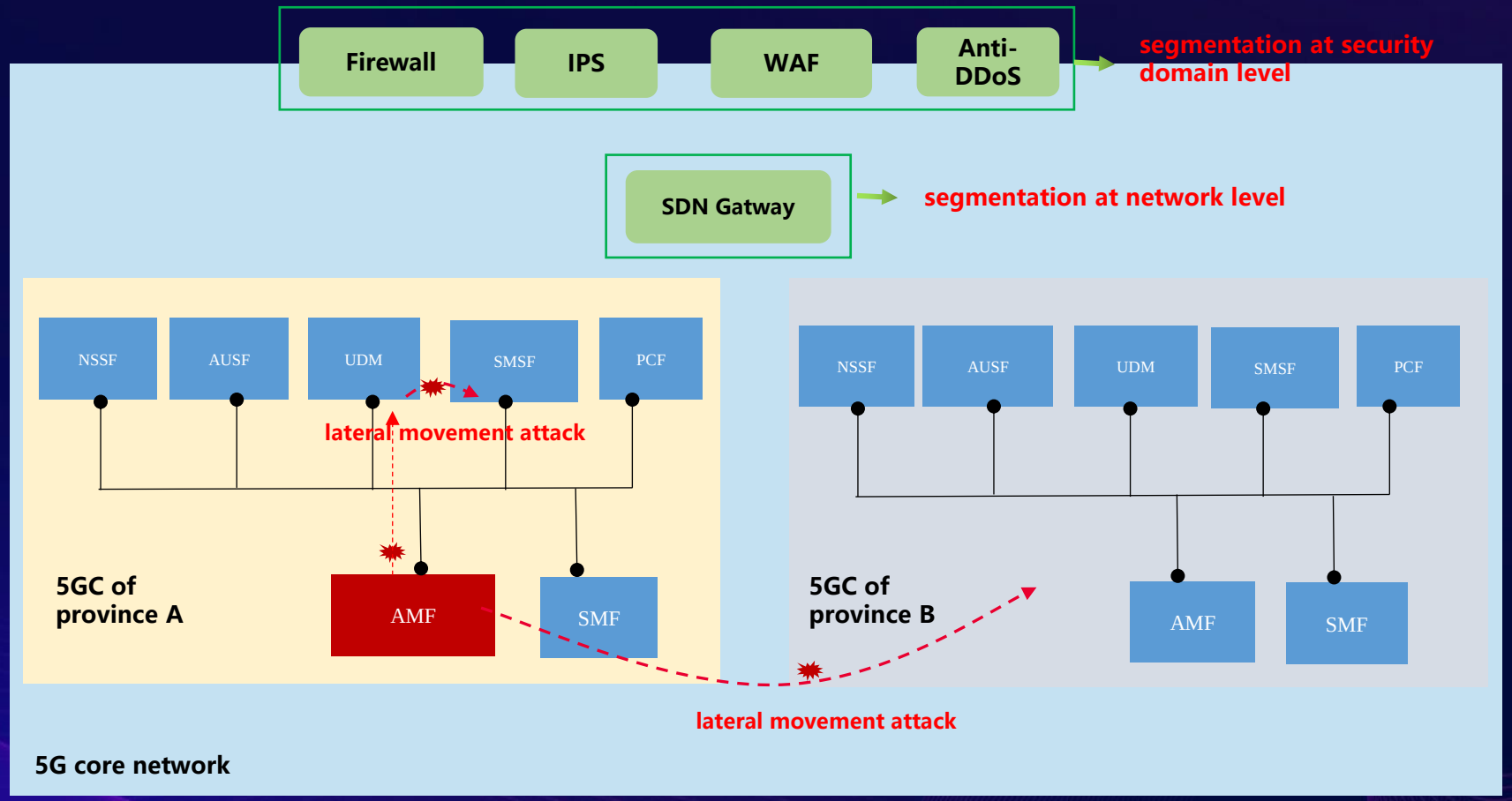
Attack path: n

Attack path: N^2 (N>>n)

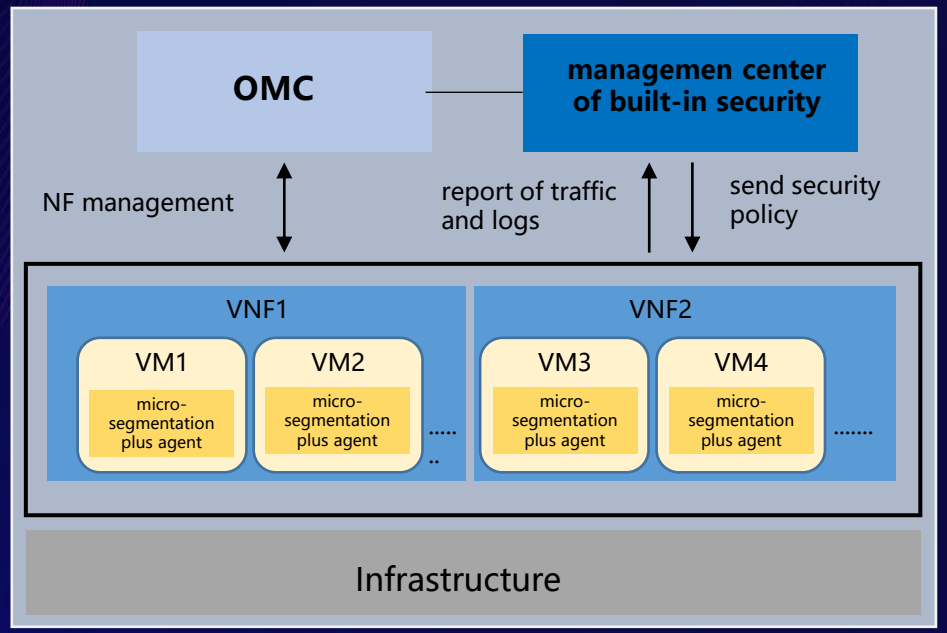
Attack path: $(N+M)^2$

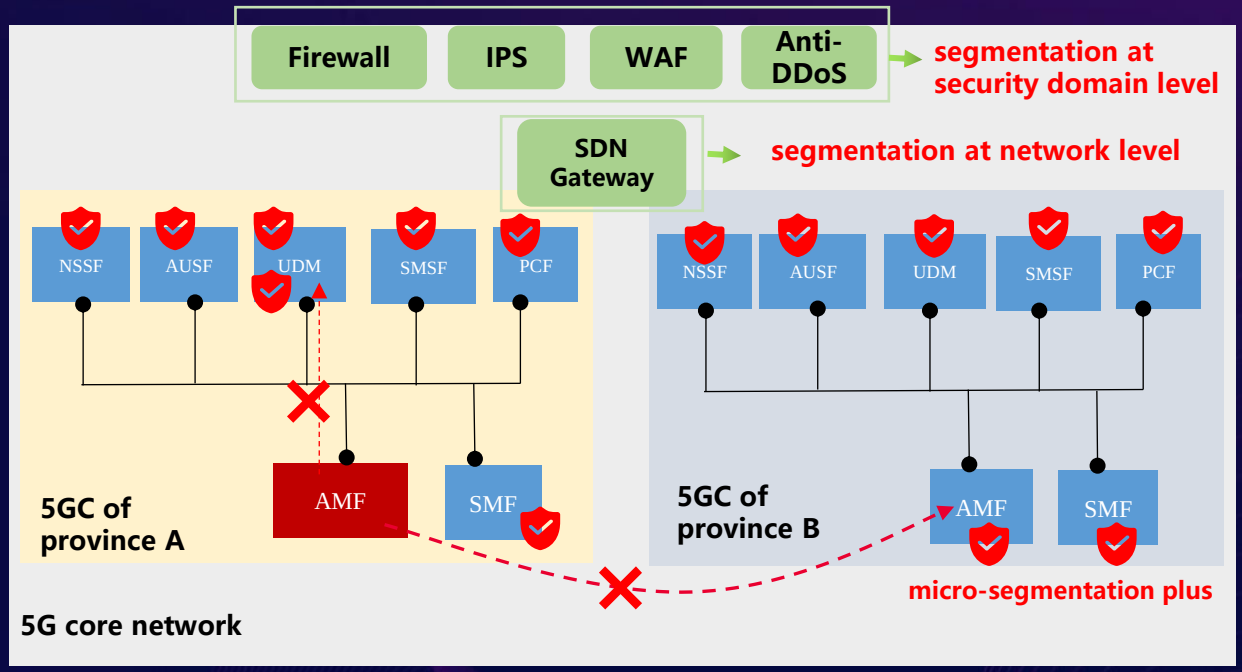
Fine-granularity segmentation is needed

Segmentation at security domain perimeter or at network level can not prevent attacks inside the domain or sub domain.



Built-in micro-segmentation plus protects intranet security of 5GC





- micro-segmentation can be deployed independently or together with NF
- intranet traffic are visible

- segmentation at VM/ container/service level
- unauthorized traffic is isolated
- intranet attacks are monitored and prevented

Funtion, performance and reliability

Built-in micro-segementation plus can achieve microsegmentation and attack awareness by 11 funtions:

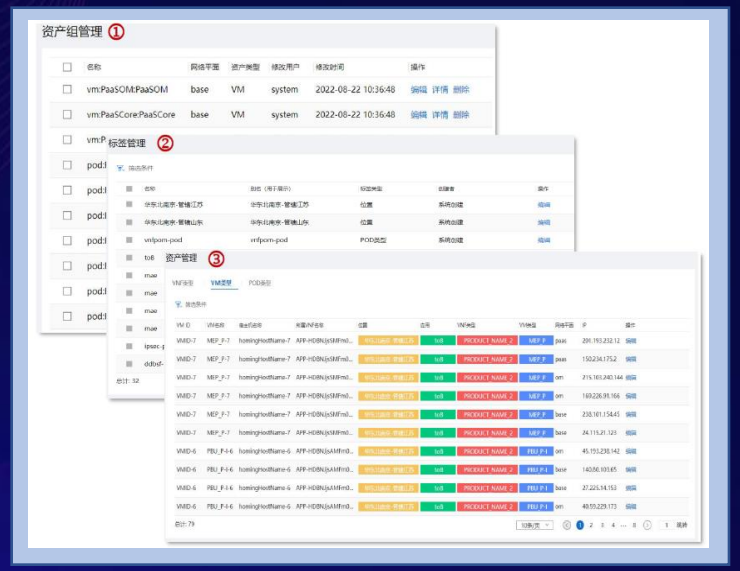
- Deployment and upgrade of management center
- one-step deployment and uninstall of micro-segementation agent
- resilient deployment of agent
- upgrade of agent
- privilege management
- assets identification
- label identification
- label management
- security policy manangement
- abnormal traffic monitoring
- traffic visualization
- detection of 15 types of attacks

9 fuctions related to performance and reliability:

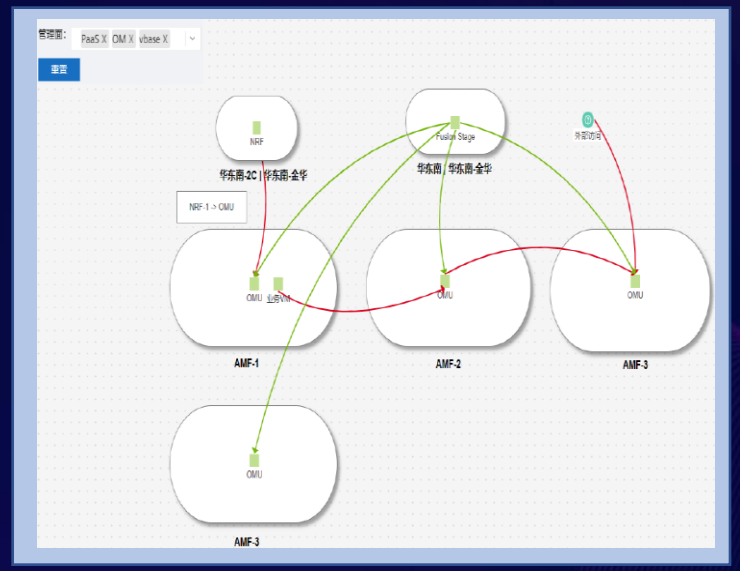
- resource usage of management center
- self healing of management center process failure
- hot backup of management center
- bypss of management center
- resource usage during agent install, running and unistall
- self healing of agent process failure
- evaluation of latency impact to network service
- self-stopping of agent
- disaster recovery

Pilot of built-in micro-segmentation plus

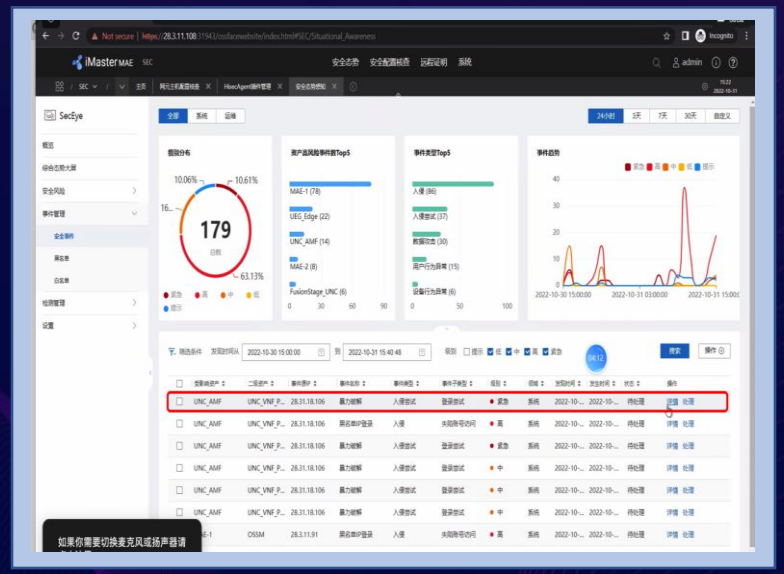
In 2023, pilot of built-in micro-segmentation plus was completed, which validates the capability of asset management, security policy management, critical file tamper etc.



asset management



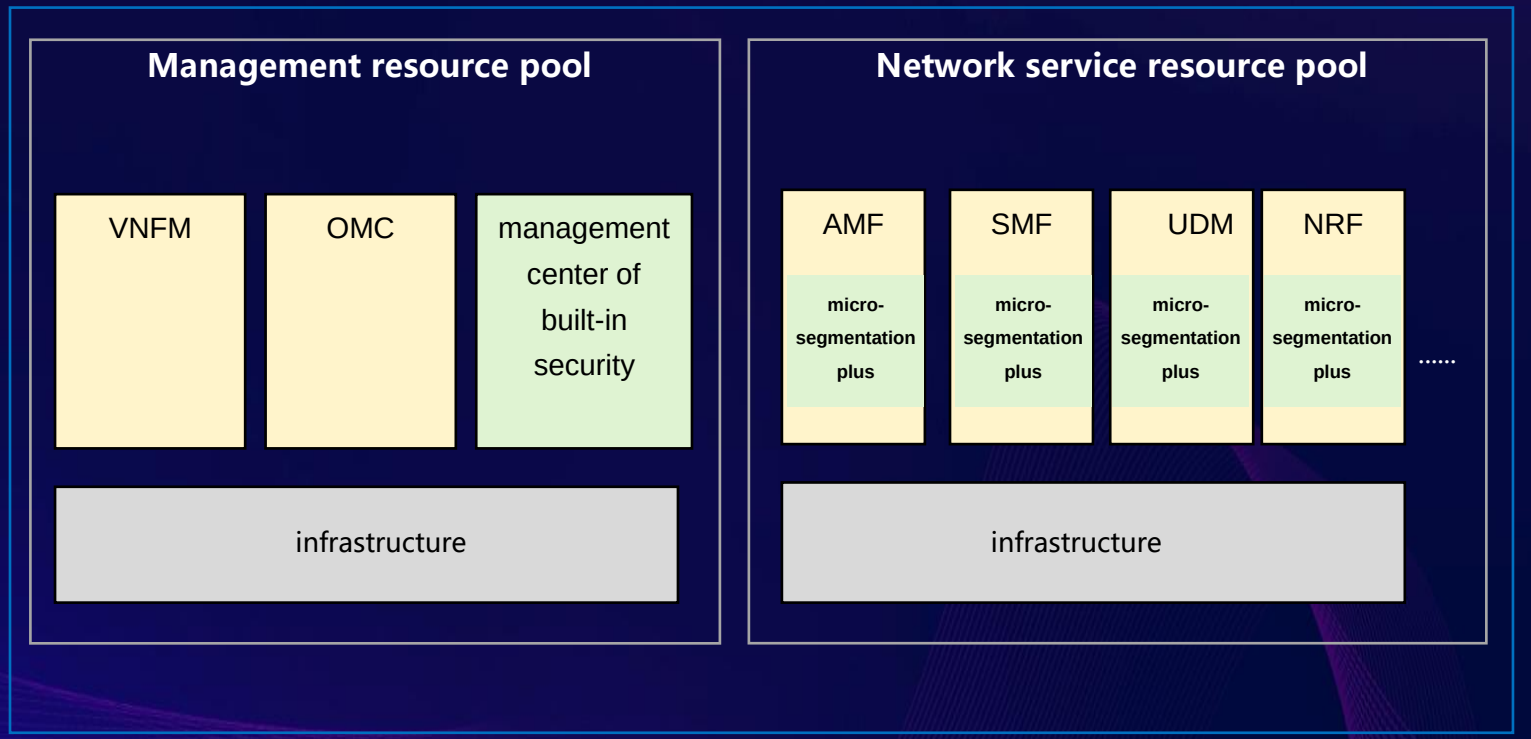
visualization of abnormal traffic



attacks statistic and logging

Advancing commercial deployment of built-in micro-segmentation plus

In 2024, China Mobile will deploy built-in micro-segmentation plus, protecting about 200,000 VMs of 5G core network functions.



Thank You

中国移动
China Mobile