Unified Safety Solution

HUAWEI CONNECT 2017

华为全联接大会

Grow with the Cloud

云领未来

Security Challenges for the City

Generalized network threats

In December 2015 and October 2016, over one million network cameras were hijacked to launch DDoS attacks.
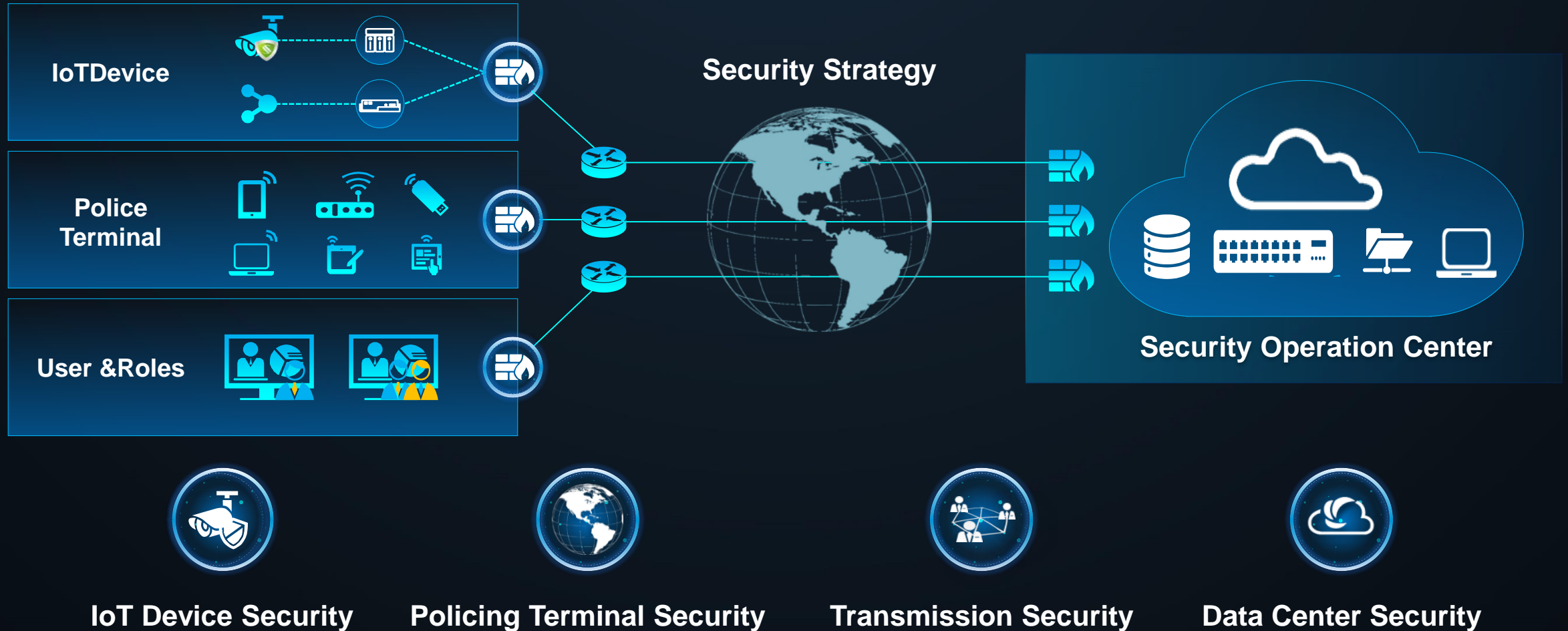
Difficulty of single-point defense

Passive defense for single points
Tired of patching the vulnerabilities
Response time to threats : 7 days
APT discovery time : 84 days

Unknown security status

Manual analysis and evaluation of asset security status
Long period of event tracing
High manpower costs

# Pre-event Detection —Full-lifecycle Security Protection For Data Information

IoTDevice

Police Terminal

User &Roles

Security Strategy

Security Operation Center

IoT Device Security

Policing Terminal Security

Transmission Security

Data Center Security

In-event Cooperation Defense — Big Data Comprehensive Analysis of Potential Threats

Analyzer

CIS (Big Data) **+** **Third-generation sandbox** **+** **Agile CONTROLLER**

Executor

FW | VPN | IPS | vFW | vIPS | DFW | 3rd安全 **+** Router | AR | WIFI | Switch | vAR | vSwitch | 探针

DATA | DATA | **Collection** | 01011101 | 1000110 | DATA | **Transmission** | **Processing** | DATA | DATA

Intelligent Detection

Passive defense→ Active defense

- MTTD: 84 days → 24 hours
- 30 hours earlier than the industry to discover zero-day vulnerabilities
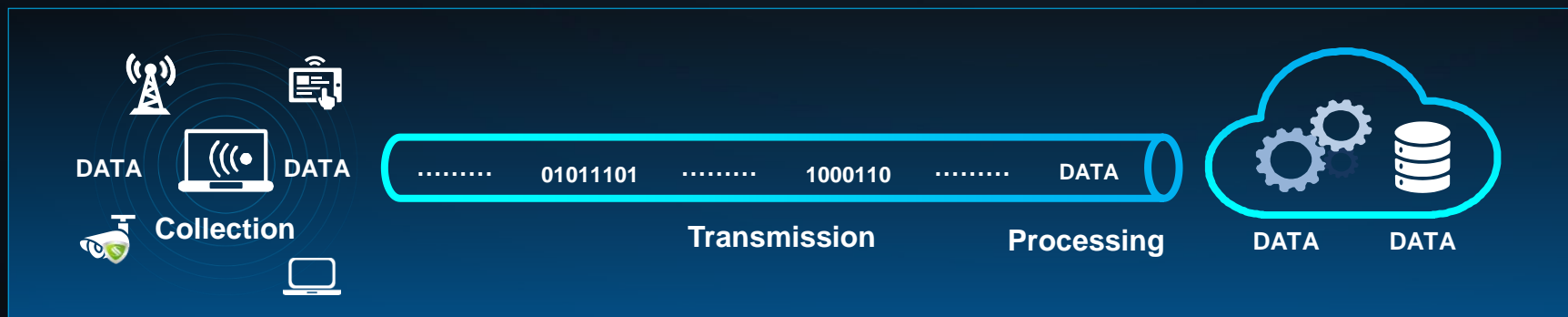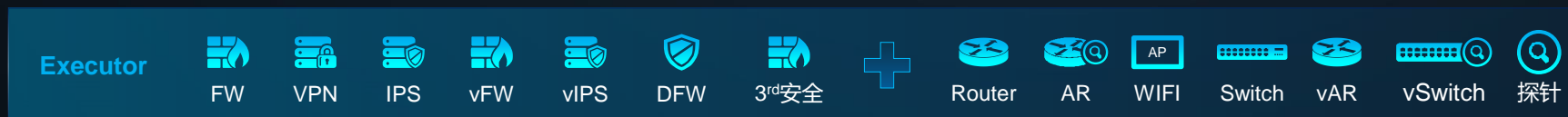
Intelligent Disposal

Single-point defense → Network-wide cooperation defense
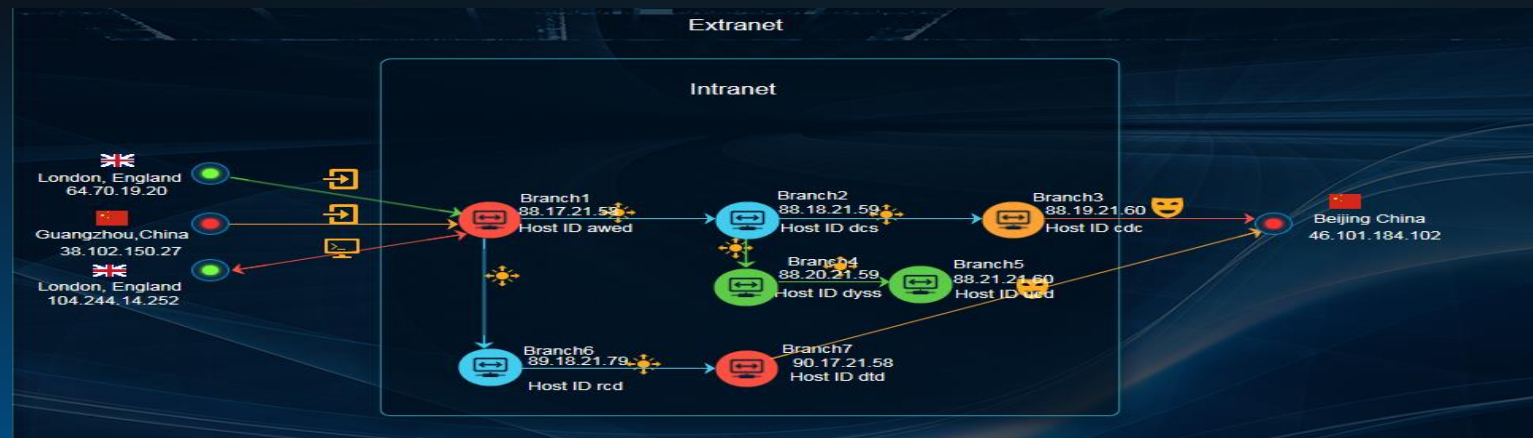
- MTTR: 7 days → 24 hours
- Network-wide device linkage blocks threats.

Post-event Audit — Comprehensive Security Reports, Source-tracing & Decision-making

Network-wide threat posture

Overall security score
Threat degrees of managed areas
Top high-risk assets
Top attack source countries
Top prioritized events

Threat Reshaping & Mining

Attack path display
Attack path display
Threat event mining
Abnormal event mining
Traffic flow mining
Log mining

Thank You.

Back