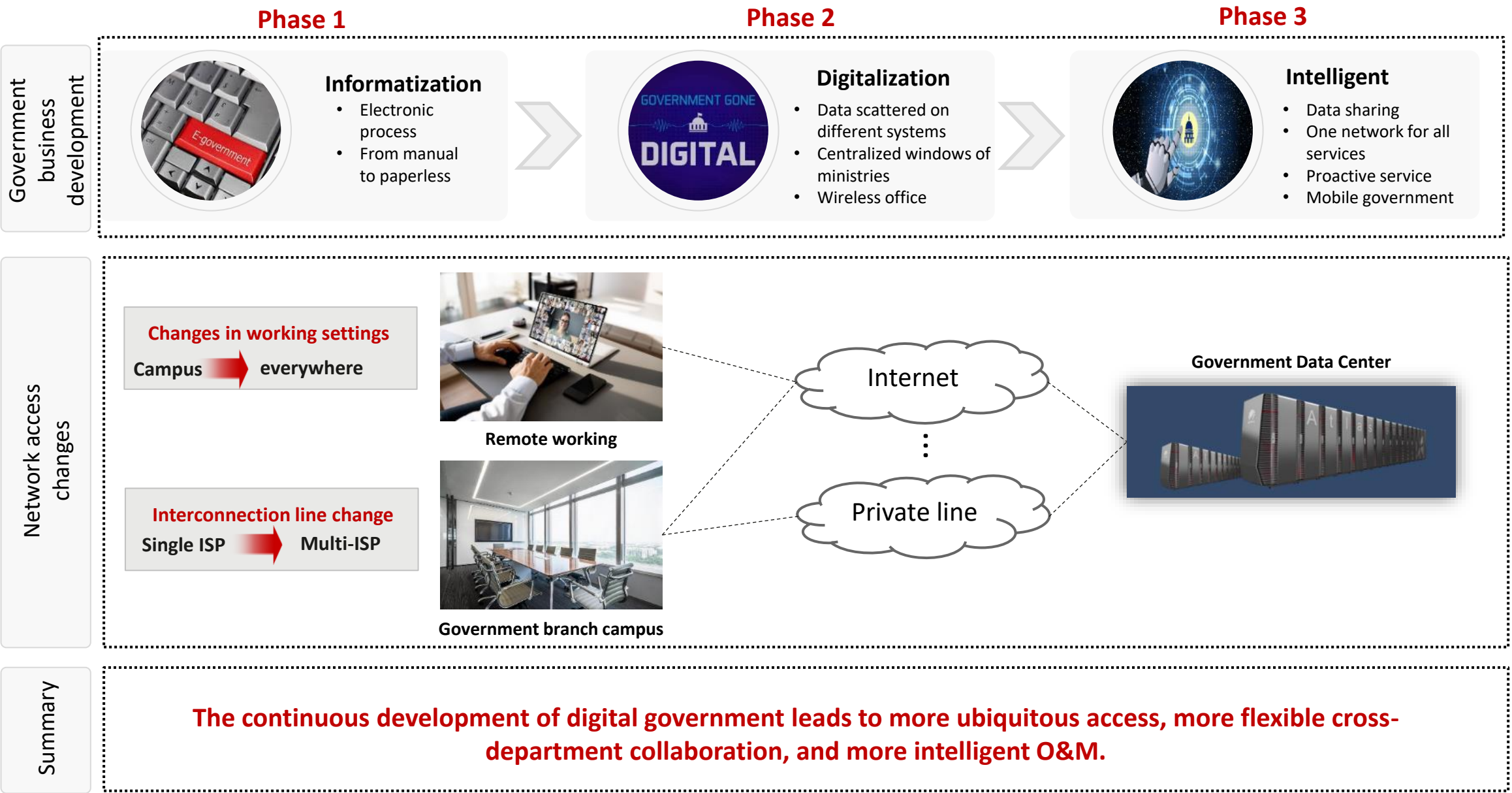


Transformation of Government Networks Through SASE Architecture

AI-Driven Cybersecurity and SD-WAN Integration in the Huawei Ecosystem



Digital Government Is Evolving Along the Path of Informatization, Digitalization and Intelligent Transformation



Major Network Security Risks and Challenges Facing Digital Government Service Development

Hindering government service efficiency



Shortage of security experts



UK: Parliament's Public Accounts Committee (PAC)
Only 4.5% of civil servants are network security experts.
Far below the average number: 12%

Secure operational efficiency needs to be improved.

Damaging government credibility



Frequent leakage of sensitive government data



Government of India
Data breach of the Aadhaar project influenced 1.1 billion people.
Increasing costs due to data breach
Security of government data transmission needs to be enhanced.

Threatening social order



Weak security capabilities of government branches



Irish Health Service Executive
Attacks on subordinate organizations spread to the HQ.
Security risks multiplied by the number of branches
Branch security capabilities need to be improved.

Government service interruption



Government service systems crashed due to ransomware



Costa Rica's Social Security Administration
Costa Rica declared state of emergency over ransomware attack
Increasing terminal security risks
Terminal security needs to be finely controlled.

Common Countermeasures Against Security Risks and Challenges in the Digital Government Industry

Improving secure operational efficiency



- Regularly provide security training for government IT technicians to improve their security awareness and skills.
- Outsource certain network security functions to professional third-party providers, such as managed security service providers (MSSPs).

Enhancing data transmission security



- Adopt efficient encryption algorithms to encrypt data during government data storage and transmission to ensure data security.
- Use mature secure transmission protocols to ensure the security of transmission channels, thereby avoiding data theft.

Enhancing the security capabilities of branches



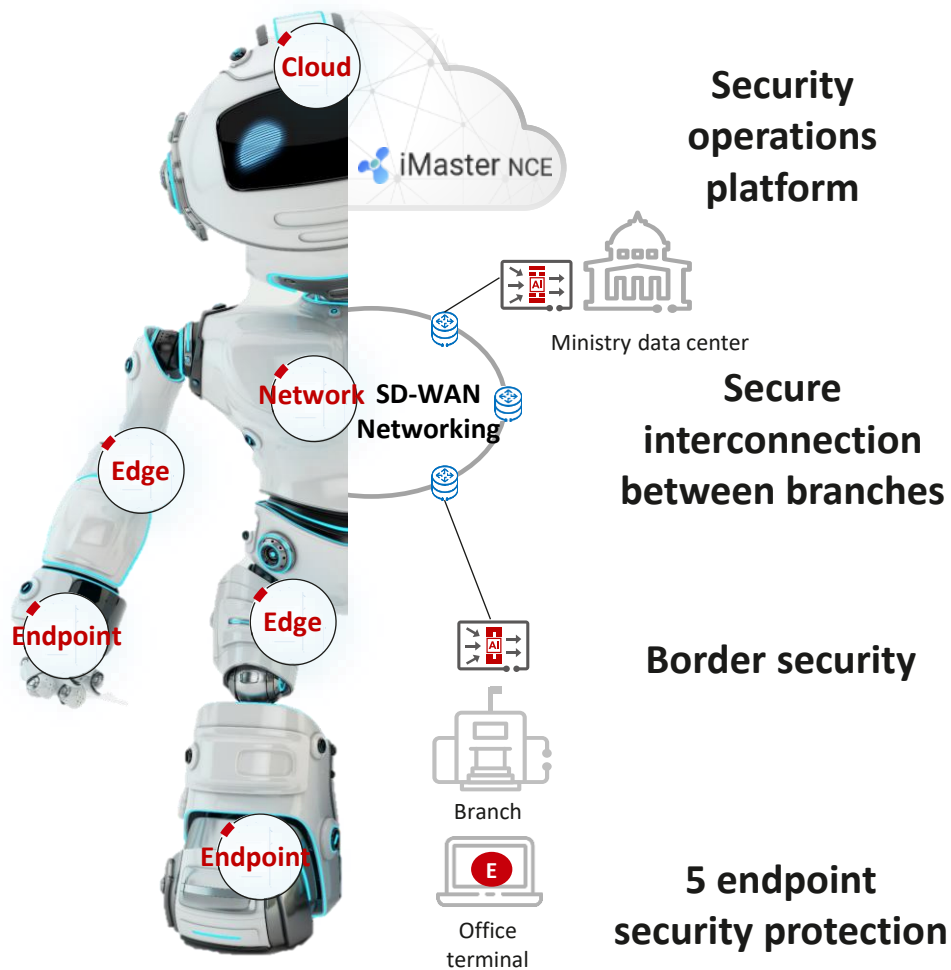
- Due to the weak technical capabilities of personnel in government branches, security products that are easy to deploy and maintain are used to simplify deployment and O&M.
- Regularly provide security training and education activities for government branch technicians to improve their security awareness and skill level.

Control terminal security in a refined manner



- Install and update antivirus software on government office terminals. Periodically scan the system to detect and remove malware.
- Use technologies, such as code, password, or MAC address authentication, to authenticate government office users. For users who use office terminals, they must pass identity authentication before accessing the campus network.

Huawei Xinghe Intelligent SASE Solution: Building a Highly Automated Security Defense System for Governments



Cloud: unified security operations and threat handling in seconds



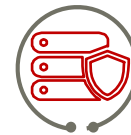
- AI-powered automatic handling of security events
- Graph engine-based accurate source tracing

Network: Secure interconnection between branches and flexible service access



- High performance, secure and efficient transmission of complex government service data
- 5G RU access, flexible branch interconnection

Edge: Efficient security protection, preventing threat spreading



- Networking-security converged devices simplify deployment and O&M, reducing TCO by 30%.
- AI-based unknown threat identification, 14% higher than the industry average

Endpoint: ZTNA and precise malware prevention

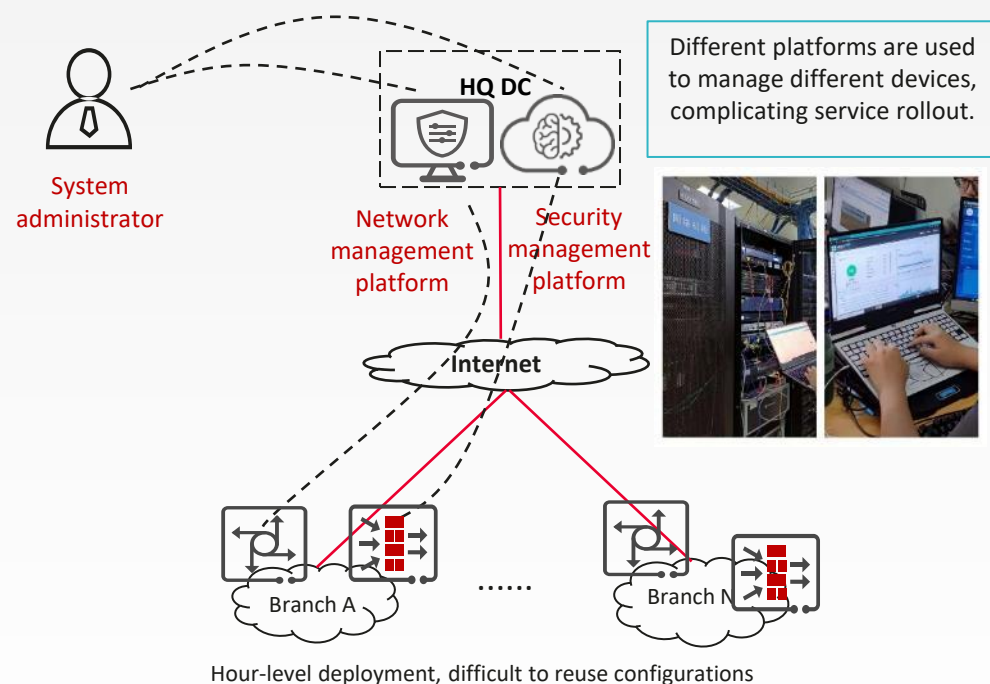


- Converged deployment, unified management, and trusted access to sensitive government services
- 100% recovery of ransomware-encrypted files based on attack behavior detection

Unified Management: Unified Network and Security Management Platform, Enabling Fast Deployment and Efficient O&M

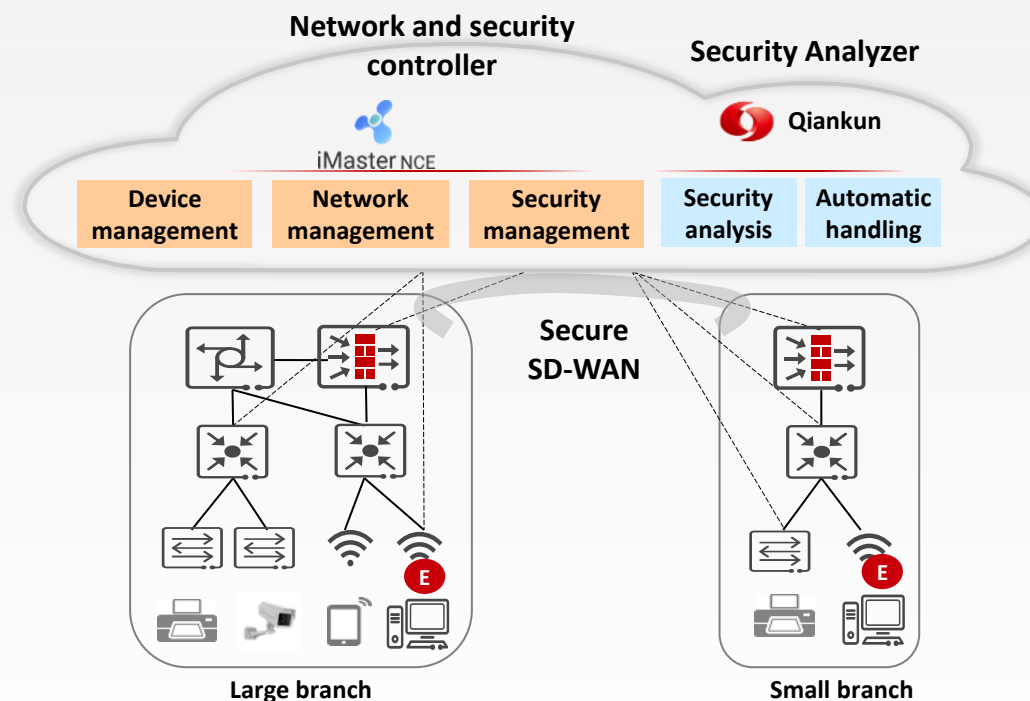
Industry Solution

The network platform, security platform, and device configurations platform are separated, resulting in high complexity and low reuse capabilities.



Benefits of Huawei Solution

Unified network and security management, control, and analysis platform helps customers quickly implement network upgrade.



Simplified deployment, building block-like construction Hierarchical template

Batch
Configuration in batches

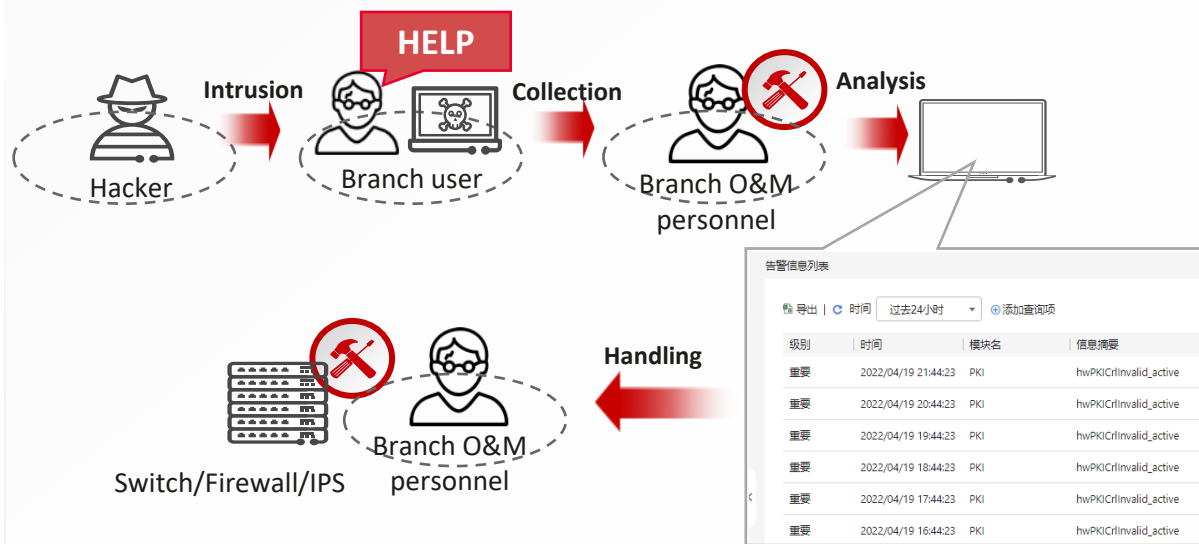
Fast
Provisioning in minutes for a single branch

85%
Efficiency improvement

Intelligent Security Operations, Automatic Handling 99% of Security Events, and Display of Network-wide Threats on One Screen

Industry solution

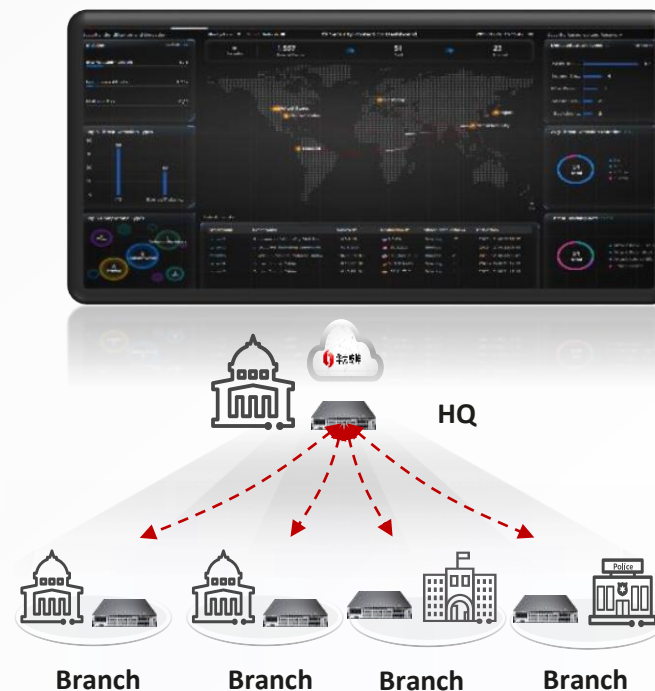
Manual threat handling, independent security management between branches



Under-staffed and under-skilled government branches are unable to handle threats promptly

Benefits of Huawei Solution

Real-time detection of network-wide threats, and automatic handling of attack events in seconds



Automatic handling of security events

80%

99%

Quick automatic handling

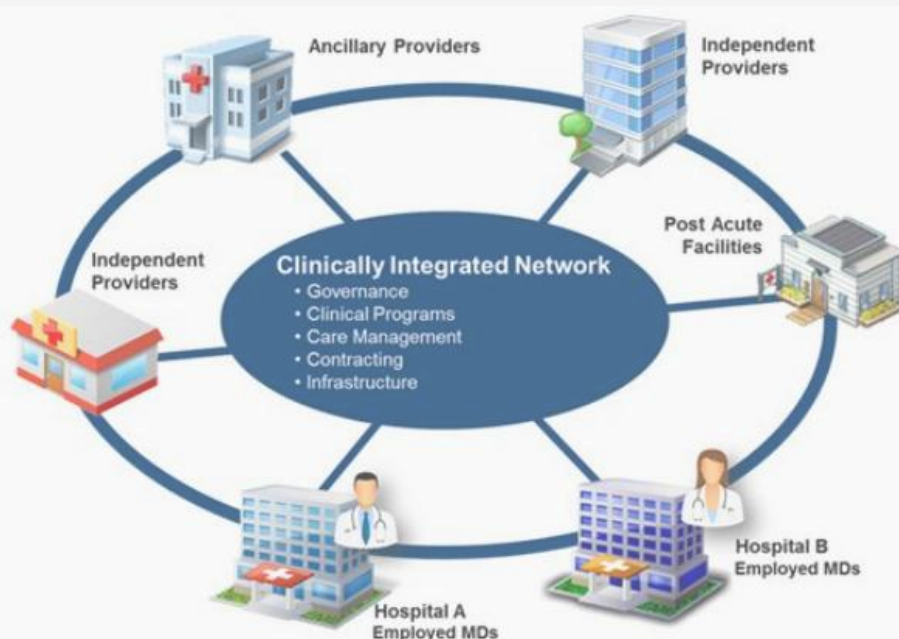
2 days

30 seconds

High-Performance Network: The High-Performance Hub Model for Secure Branch Networking, Tunnel Encryption, and Threat Prevention

Scenario and Challenges

- ✓ Customer requirements: The XXX healthcare department has 1000 branches. Multiple branch networks are interconnected for office and branch video security backhaul. Each branch has 10 cameras. Each camera requires 4 to 8 Mbit/s bandwidth. The uplink bandwidth of each branch is 100 Mbit/s. The interconnection bandwidth between the headquarters and branches must be 100 Gbit/s.



Competitiveness & Value of Huawei's Solution

In-depth software and hardware collaboration, resulting in 75% higher tunnel encryption forwarding performance



Highway

Dedicated lane, non-blocking forwarding

Application traffic

1 2 3

High-priority vehicle



Fast lane

1 2 3

Regular vehicle



Slow lane

Application traffic

Forwarding coprocessor

Proprietary NP forwarding engine

Service Accelerator

SSL service acceleration engine

FEC engine

TCP acceleration engine

Pattern matching engine

Encryption/Decryption algorithm engine

Traffic management engine

AI engine

Efficient data transmission encryption

55 Gbps

Industry

96 Gbps

Huawei

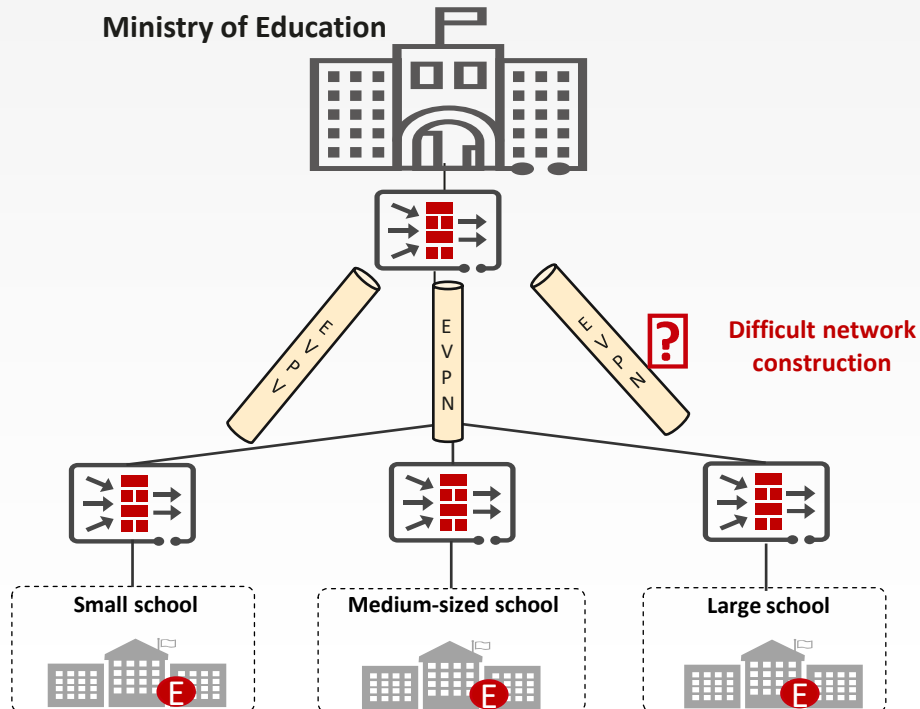
High-performance hub SD-WAN tunnel performance



Flexible Access: 5G to support management

Scenario and challenges

- ✓ Customer requirements: The XXX Ministry of Education needs to interconnect 4K+ schools. More than half of the schools are located in remote areas. As a result, network construction is difficult and costly. Deploying 5G wireless network can significantly reduce construction cost and construction period.



Competitiveness & Value of Huawei's Solution

Portable and Efficient 5G Networking, Rapid Digitalization of Main Services



A 5G-RU functions as a remote unit of a firewall and is configured and managed by the firewall. The 5G-RU enables a branch to establish a connection with the headquarters over the Internet through a 5G wireless link.

Fast deployment

RU-201 management and control as well as email-based deployment on the controller

Real-time monitoring

An alarm is generated when the link between the RU and the FW is disconnected.

Flexible networking

A single firewall supports a maximum of four RUs.

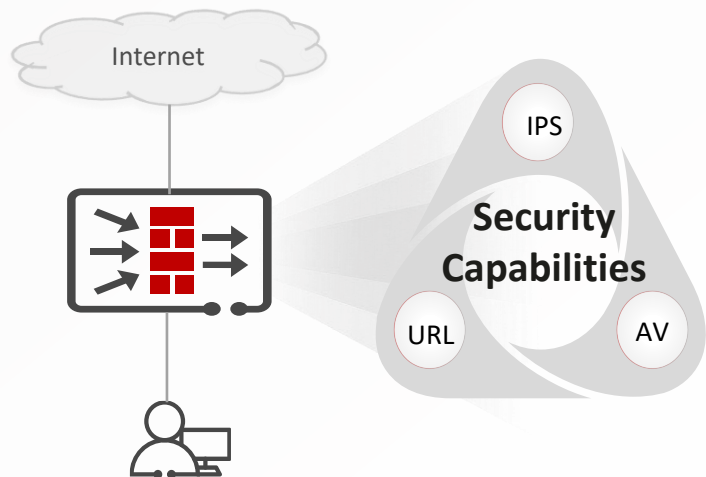
Easy deployment

The device can be connected to the GE/10GE/25GE/40GE electrical interface of the firewall.

Defense Against Unknown Threats: AI-powered Unknown Threat Identification, with a Detection Rate of 95%

Industry solution

Static threat detection using a threat database, which is updated periodically

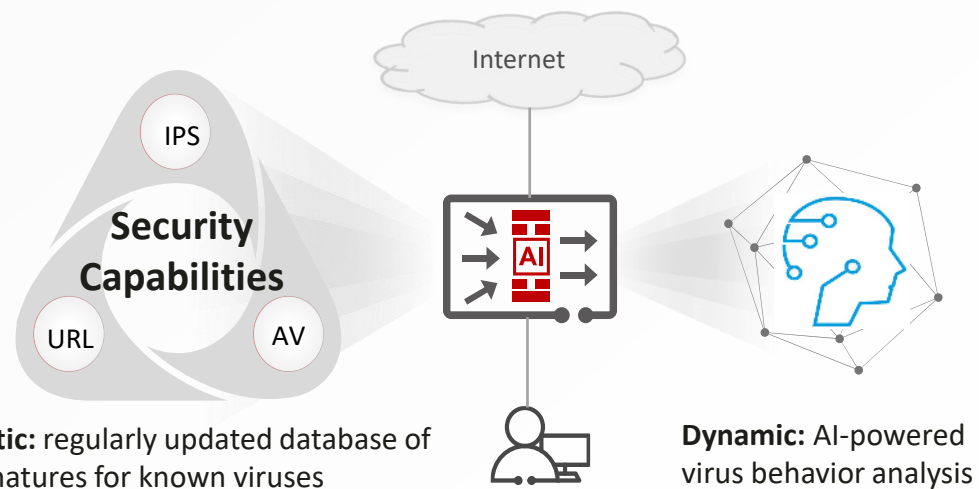


Due to AI technologies, 120 million new malware variants are generated each year.

Static detection based on the antivirus signature database cannot cope with rapidly increasing new variants.

Huawei solution & benefits

Static threat detection + dynamic AI-powered unknown threat detection



Static: regularly updated database of signatures for known viruses

Dynamic: AI-powered virus behavior analysis

Blind test using MalwareBazaar, a well-known public virus signature database

Detection rate (industry)

80%

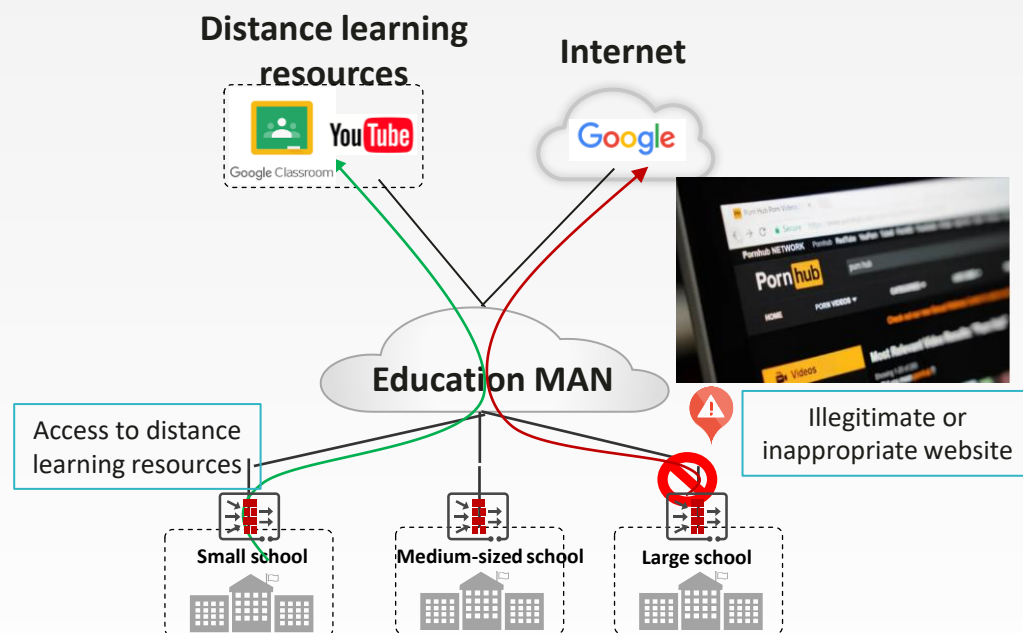
Detection rate (Huawei)

95%

Safe Internet Access: AI-powered Precise Blocking of Malicious and Inappropriate Websites to Ensure Internet Safety for Minors

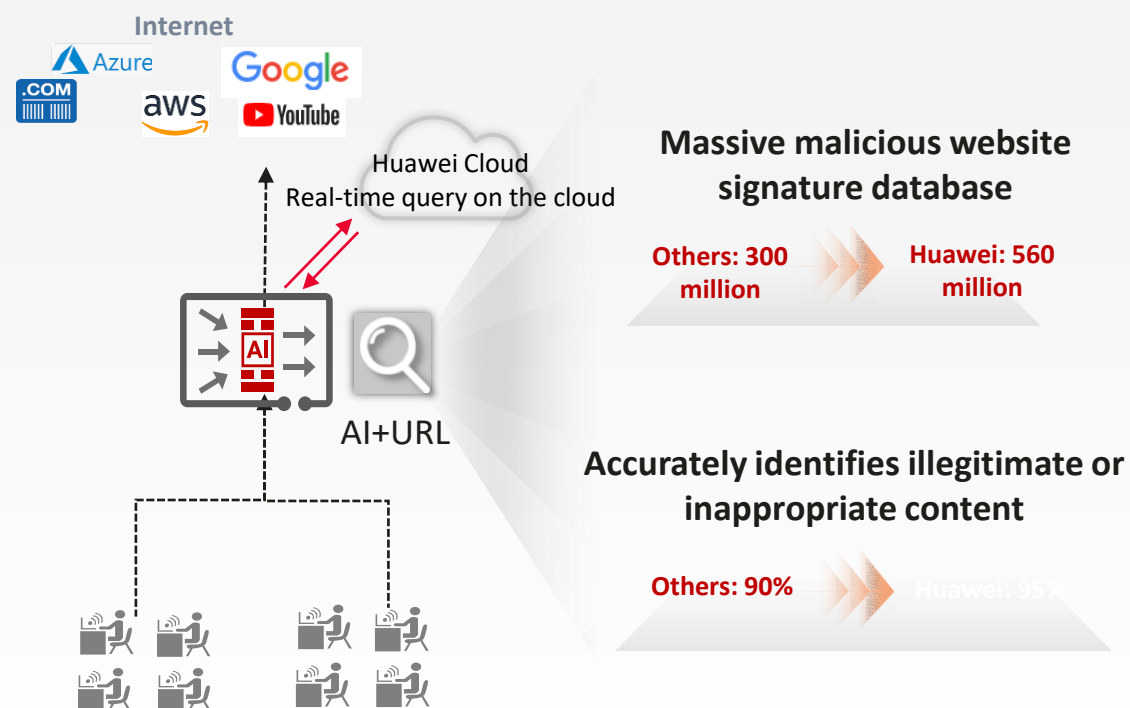
Scenario and challenges

Challenges: Inappropriate content pops up during multimedia instruction, interrupting class activities.



Competitiveness & value of Huawei's solution

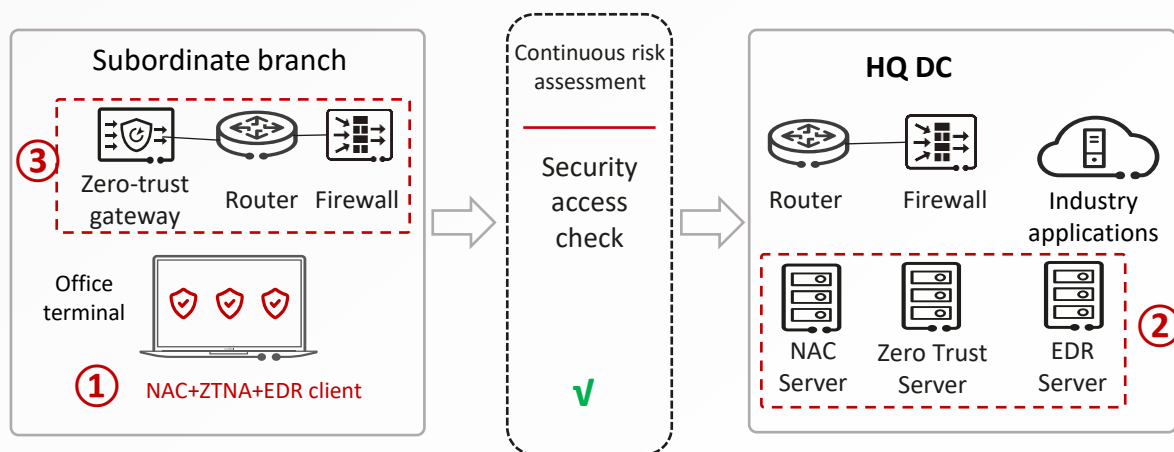
AI-powered smart gateways accurately block malicious websites to ensure Internet safety for teachers and students.



Zero-Trust Government Access: Dynamic Access Authorization for Dual-Purpose Devices, Ensuring Service Data Security

Industry Solution

Zero-trust deployment, O&M, and management are complex, and authentication policies are not unified.

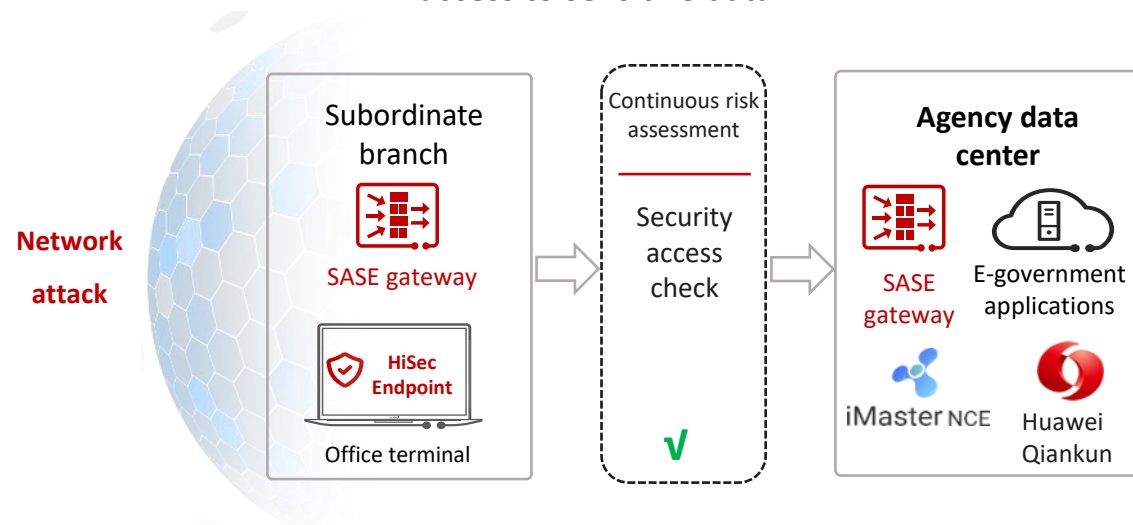


①② The NAC, ZTNA, and EDR components are deployed independently, increasing terminal resource usage and complicating management and O&M.

③ Multiple access devices need to be deployed on a branch campus network. The deployment is complex, the cost is high, and the network delay is long due to traffic detour.

Huawei Solution & Benefits

Converged deployment, unified management, and trusted access to sensitive data



Three-in-one client and integrated deployment reduce OPEX by 70%

Unified authentication and policies

One device with multiple functions, simplifying deployment and O&M and reducing TCO by 30%

NAC, ZTNA, and EDR

HiSec Endpoint

Independent certification and policy

iMaster NCE

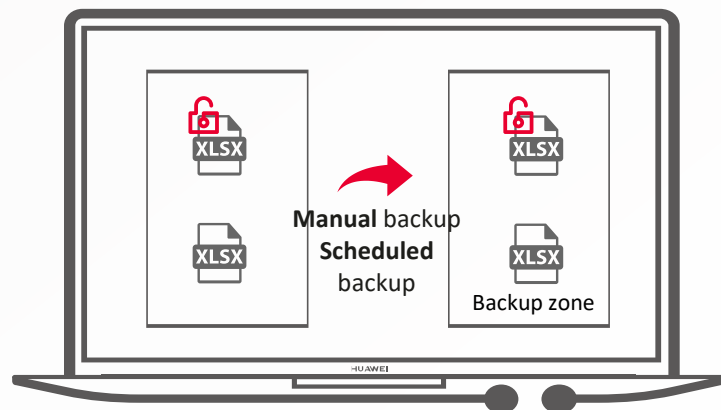
Firewall, router, and zero trust

SASE gateway

Ransomware Protection: Virus Protection Based on Attack Behavior Detection and Dynamic File Backup

Industry Solution

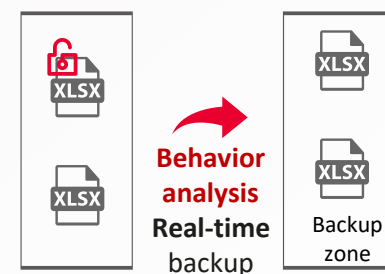
To prevent ransomware attacks, critical files are periodically backed up.



Backup is triggered periodically. The ransomware and normal files are backed up and restored together.

Benefits of Huawei Solution

With AI-powered behavior analysis, file backup is triggered only when potential attack is detected.

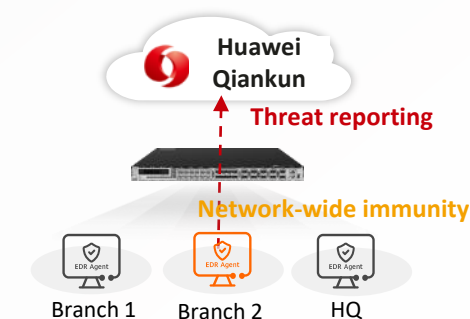


Only files that will be encrypted by the ransomware are backed up.

Anti-ransomware to ensure 0 data loss

Manual/Scheduled backup

Automatic backup and one-click restoration



One-click ransomware rollback and collaborative handling

Collaborative defense and network-wide immunity

Single-point defense

Protection on the entire network upon detection on one node

Huawei Xinghe Intelligent Unified SASE Solution

Building a Multi-branch Security System

Cloud



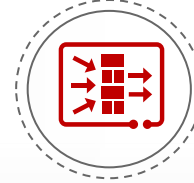
Unified security operations and threat handling in seconds

Network



Secure interconnection between branches and flexible service access

Edge



Efficient security protection, preventing threat spreading

Endpoint



ZTNA and precise malware prevention

Analyzer



**Huawei
Qiankun**

Qiankun-OP

Network-wide security situational awareness and threat detection in seconds

Controller



iMaster NCE

iMaster NCE-Campus

iMaster NCE

Unified management of network and security devices and integrated O&M

SASE gateway



USG6500F



USG6600F/USG6700F

HiSecEngine

High-performance converged security gateway

Endpoint security client



HiSec Endpoint

Efficient threat detection and lightweight deployment

Multiple International Awards and Certifications

AV-TEST: advanced threat prevention certification



SASE solution certified by Tolly



SKD Labs: 100% known threat detection



Recommended SASE supplier by Forrester for 2 consecutive years



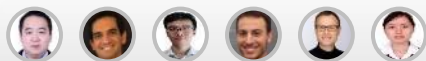
Huawei firewalls have been listed in Gartner Peer Insights Customers' Choice with a high score for 3 years in a row



Huawei Security - 25 Years of Expertise and Continuous Development Innovation

6 security technology labs

5 R&D teams



2500+

Security R&D professionals



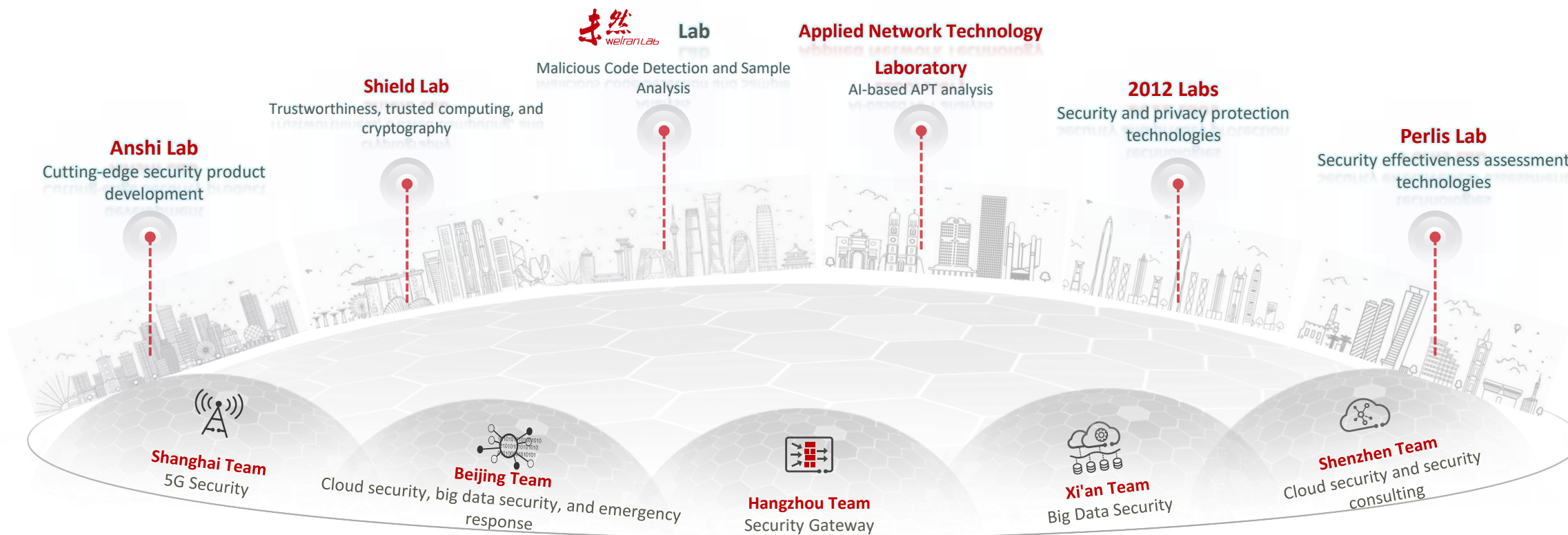
CNY10B

**Security R&D investment
per year**



3000+

**Security patents (chips, AI,
etc.)**



Huawei Xinghe Intelligent Network

Unleashing digital productivity and diving into intelligence in all industries



Government



Finance



Education



Manufacturing



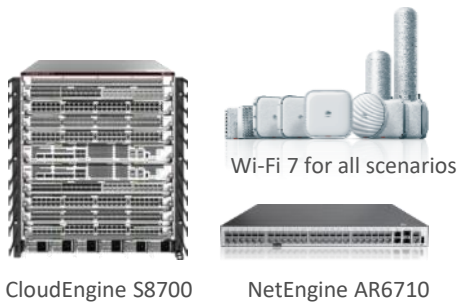
Transportation

...

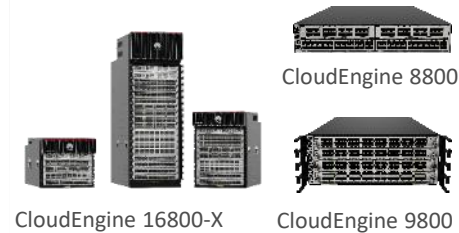


Energy

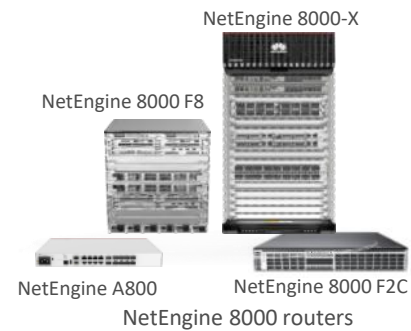
Xinghe Intelligent Campus



Xinghe Intelligent Fabric



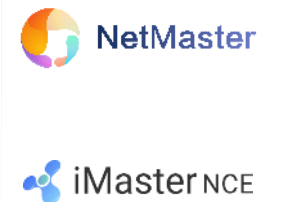
Xinghe Intelligent WAN



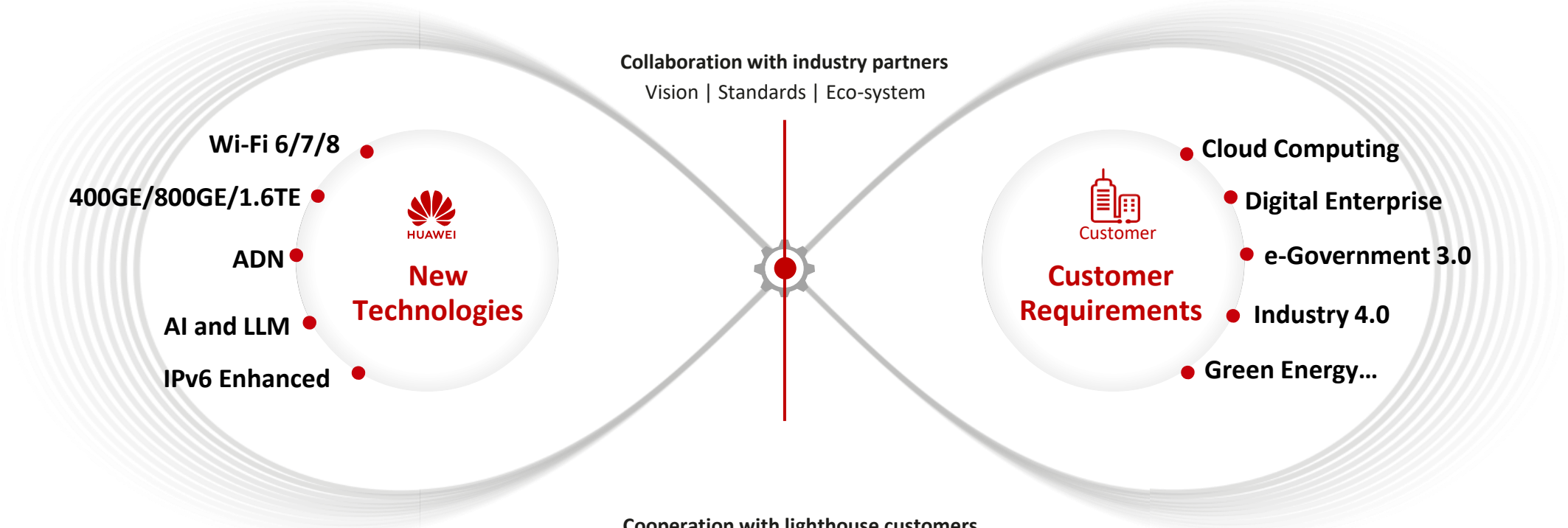
Xinghe Intelligent Network Security



NetMaster



New technologies & customer requirements driving network innovations





Net5.5G Network Foundation for the Intelligent World

AirEngine Wi-Fi 7 | CloudEngine Switches | NetEngine Routers | HiSecEngine Security Gateways

Thank you.



Building a Fully Connected, Intelligent World