AIFW, Empowering Future Enterprise Security with AI

Huawei HiSecEngine USG6000E Series AI Firewall Technical Presentation

V600R007

Security Level:

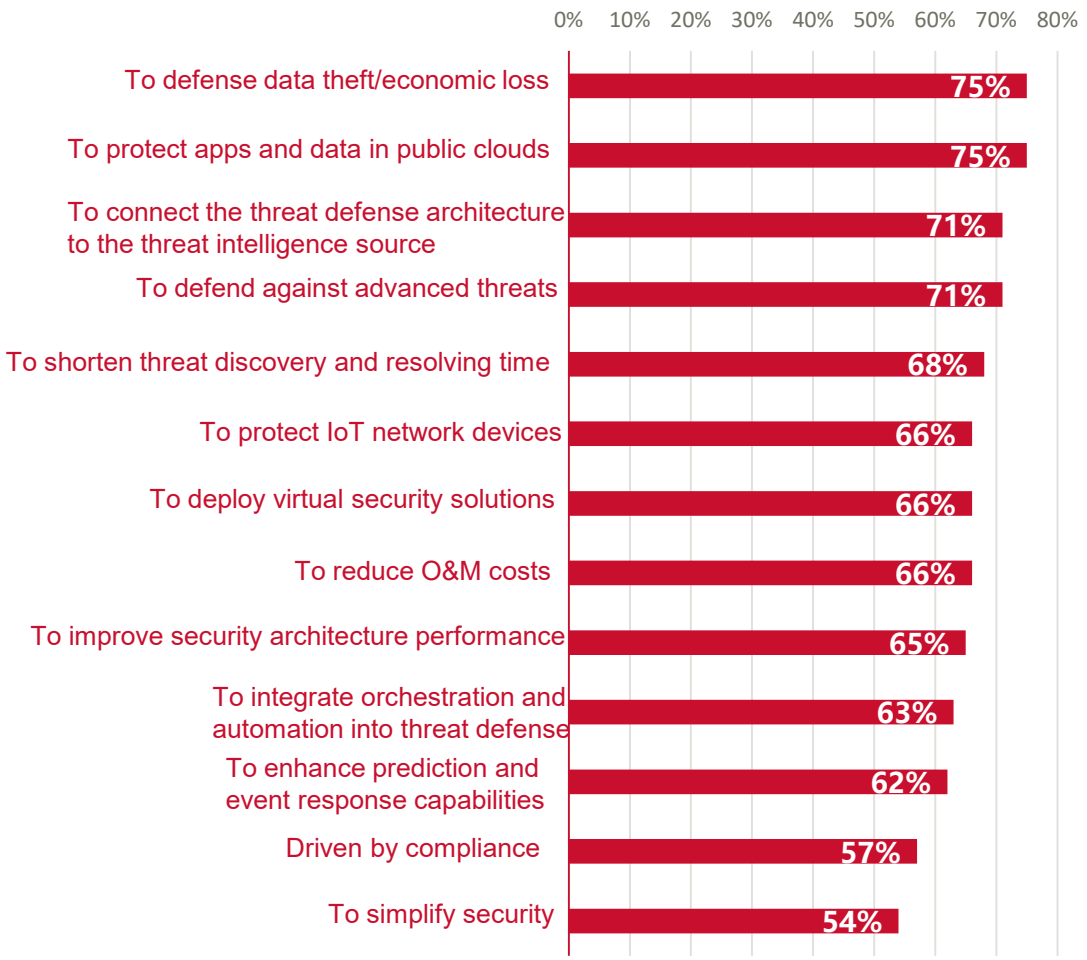
HUAWEI

Contents

Security: Objectives and Obstacles of Security Deployment

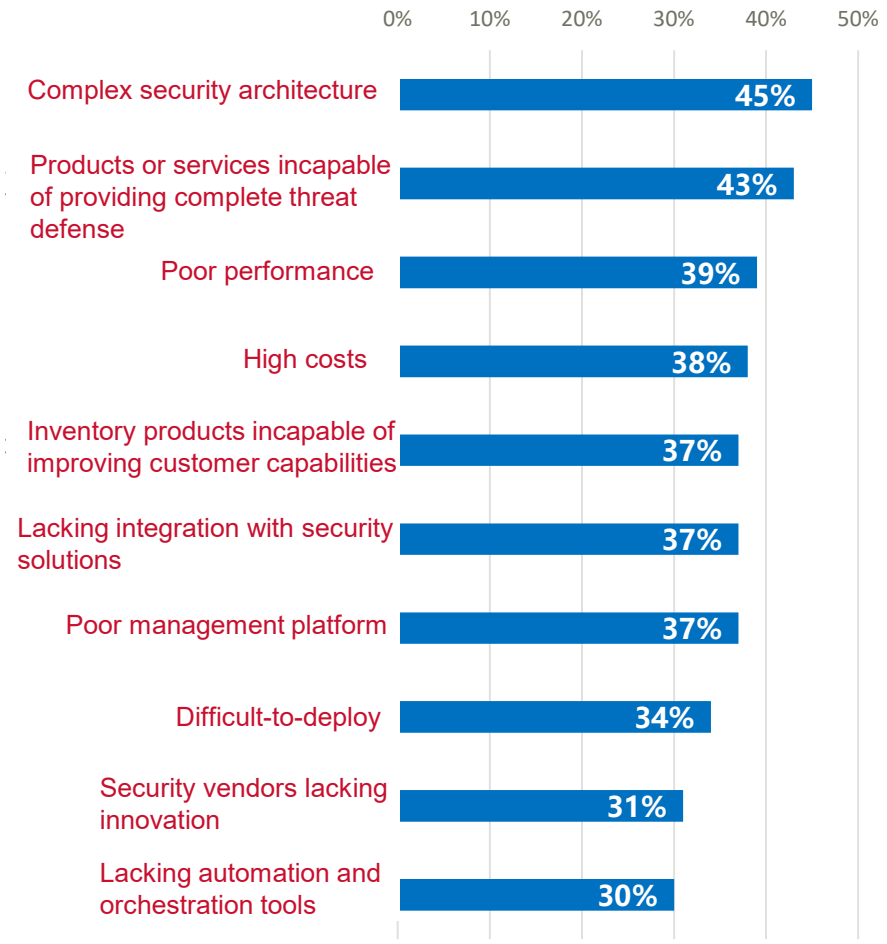
Objectives of security deployment:

To protect core data, defend against advanced threats, shorten the threat processing time, and reduce O&M costs



Obstacles to security deployment:

Complex deployment, low cost-effectiveness, far from helping customers shorten the threat identification time



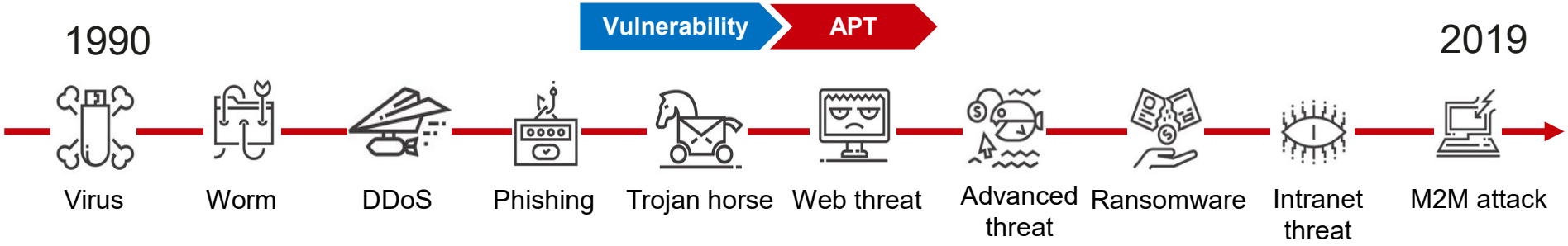
Source: IHS 2019

Threats: Ever-Changing, More Difficult to Be Detected by Traditional Firewalls

Fast-changing threats

↓

More difficult in protecting the network



Frequent threat variation

↓

The traditional signature database is slow in detecting and responding to threats

GlobeImposter: four variants in 2 years, ever-changing encryption algorithms and file suffixes

Warnnacry: various variants in 2 months

Multi-dimensional attacks, increasing encrypted services

↓

Difficult in detecting attacks

In 2017, internal threats accounted for 34%, which increase year by year.

Source: Verizon

In 2019, 75% of web traffic is encrypted.

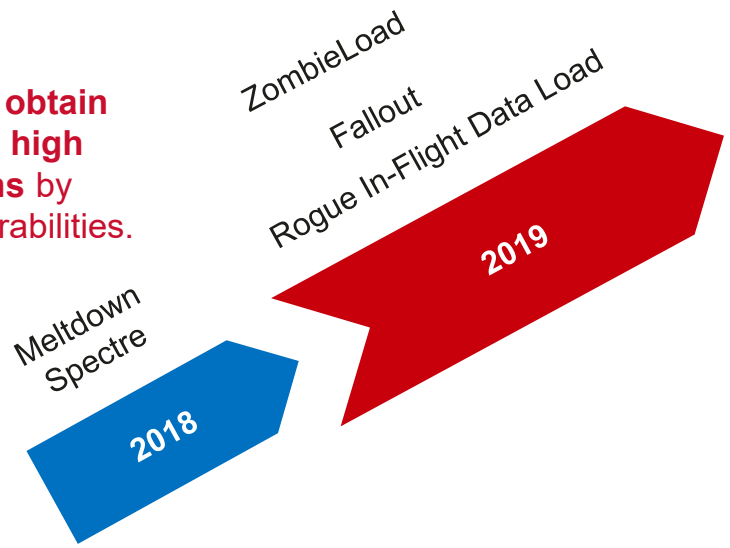
Source: NSS LABS

Products: Universal and Home-Made Chips, To Be Improved

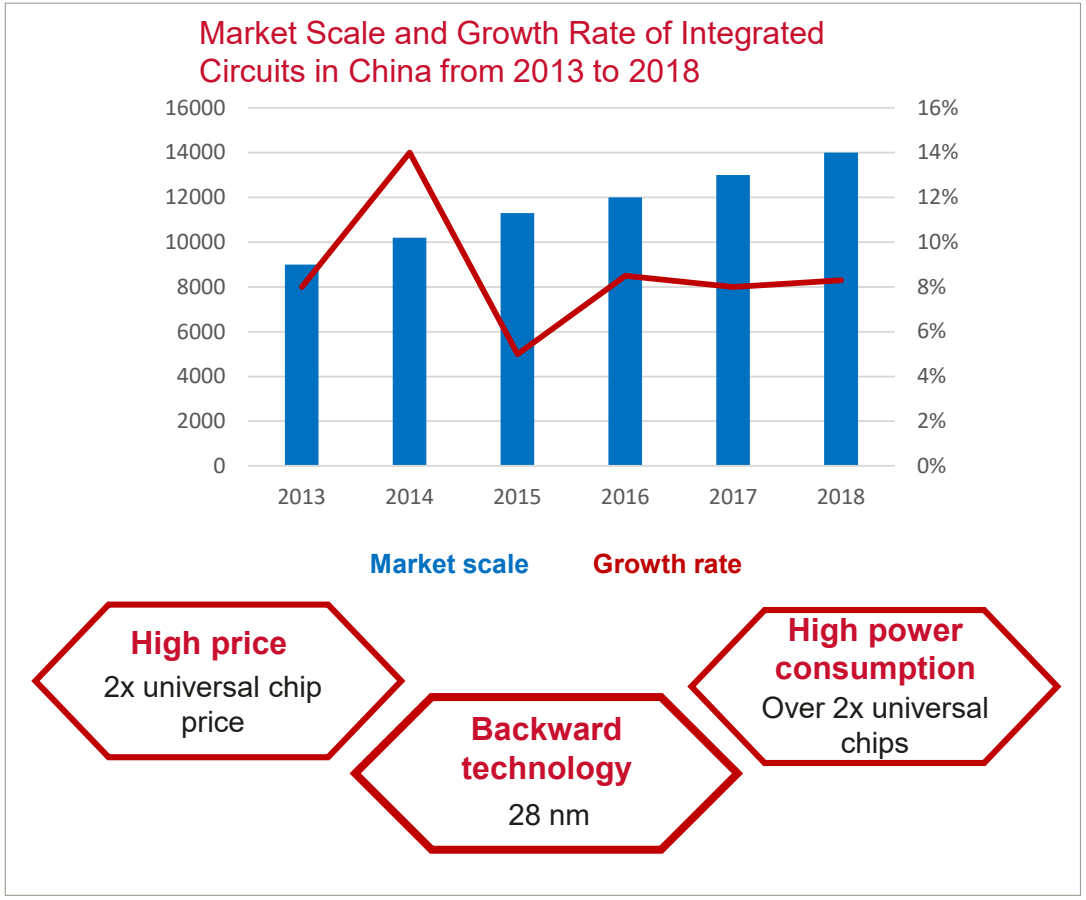
Intel chips open the "Pandora's Box" of chip vulnerabilities

All data loaded to the processor core is **leaked**

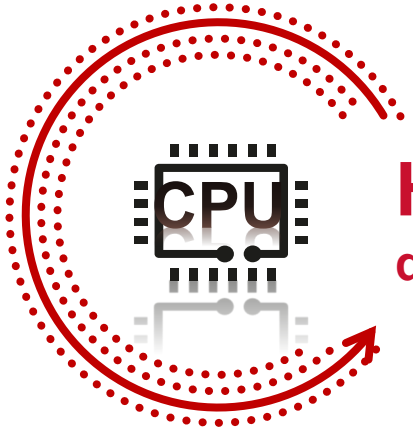
Attackers can **obtain kernel-level high permissions** by exploiting vulnerabilities.



Home-make chips are still developing

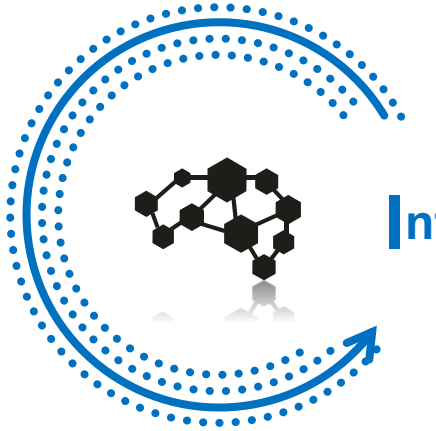


What Kind of Firewall We Need?



Huawei-developed chip

- **Huawei-developed security chip**: Built-in co-processing engine (forwarding/encryption/pattern matching acceleration)
- **Huawei-developed AI chip**: 8 TOPS 16-bit floating-point computing power, supporting advanced threat defense pattern matching acceleration



Intelligent defense

- **Three threat defense engines:**
  - **Next-generation engine (NGE)**: IPS/AV/URL NGFW detection engine
  - **Cloud deploy engine (CDE)**: malicious file analysis engine
  - **Artificial intelligence engine (AIE)**: APT threat detection engine

New

New

Simplified O&M

New

- **New web UI 2.0**
  - A new security UI supporting threat visualization
- **CloudCampus Solution**
  - Fast and simple network deployment
  - Security controller integrated into Agile Controller-Campus as a component, enhancing firewall O&M and management

New

Contents

Huawei-Developed: All Core Chips and Core Software Are Developed by Huawei

CPU with industry's best security defense capability

NPU with industry's best forwarding capability

AI system-on-a-chip (SoC) with industry's highest edge computing capabilities

- **Chip:** Use Huawei-developed key chips to build core competitiveness.
- **Capability:** Construct industry-leading basic hardware and manufacturing capabilities.

Device operating system (OS)

Network OS

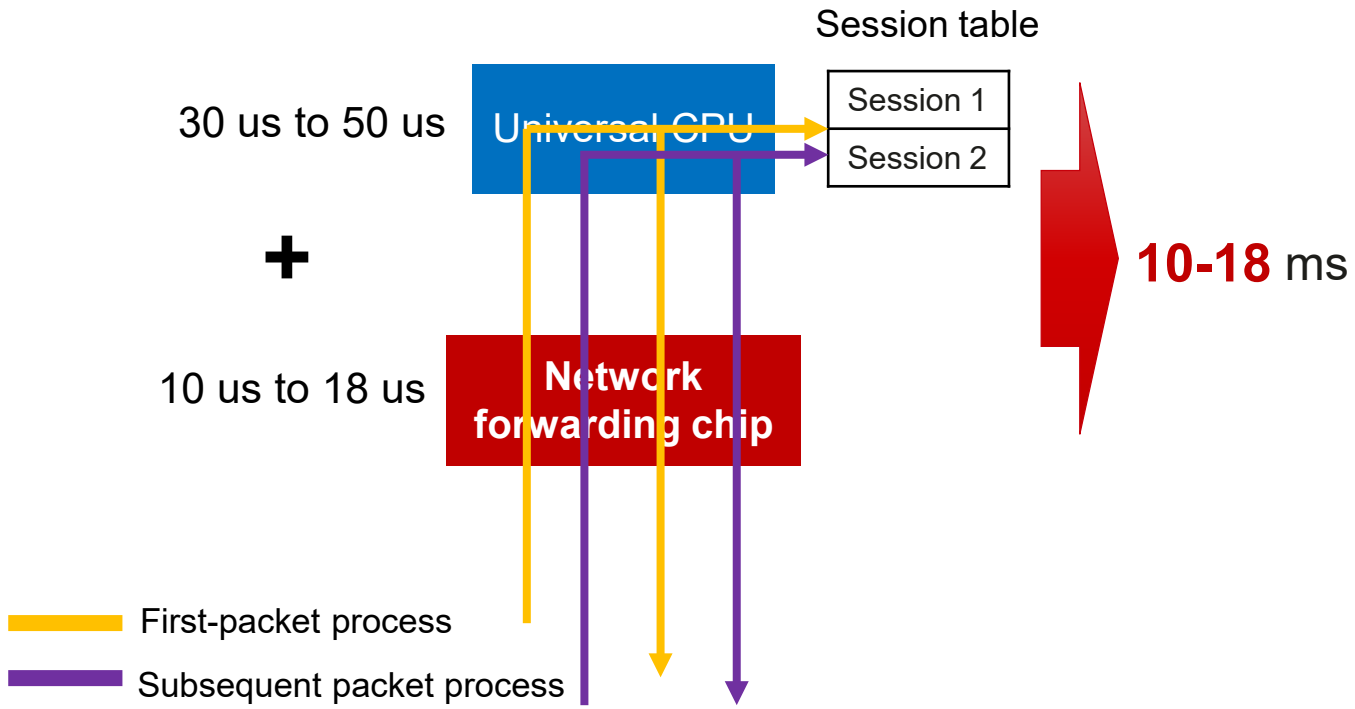
International standards

- **OS:** Huawei-developed and customized OSs for communication networks, providing better performance and functions.
- **Standards:** Proactively participate in and lead standards innovation.

Huawei-Developed: Unloading Data Services from Huawei-Developed Chips, Implementing Low-Latency Forwarding

As-Is

High latency:
Network chip processing latency + computing chip processing latency = Total latency of a traditional firewall

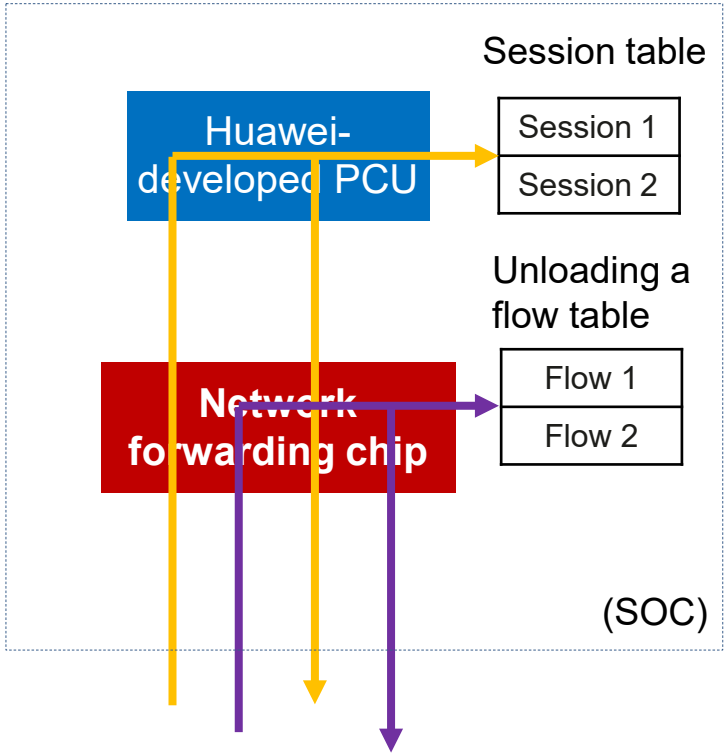


10-18 ms

To-Be

Lower latency:
Huawei firewalls unload session entries through network forwarding chips (low-end SOC integration), reducing the packet forwarding latency by 70%.

Customized packet forwarding acceleration:
Huawei firewalls can customize packet forwarding acceleration based on ACLs/interfaces, protecting key services.



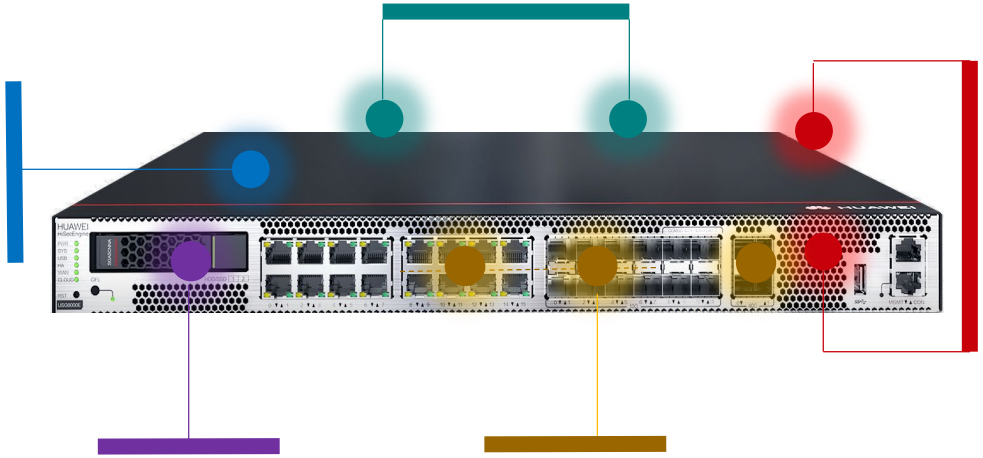
Huawei-Developed: USG6000E, Meeting Various Customer Requirements

High reliability

- Dual power redundancy and 3+1 fan module redundancy

Intelligent frequency conversion, saving power

- Automatic adjustment of power consumption based on the port status, 30%↓ power consumption
- Adaptive voltage scaling (AVS), effectively reducing the chip power consumption



Data center-specific

- Front-to-back ventilation, meeting data center requirements
- 1 U height, saving rack space

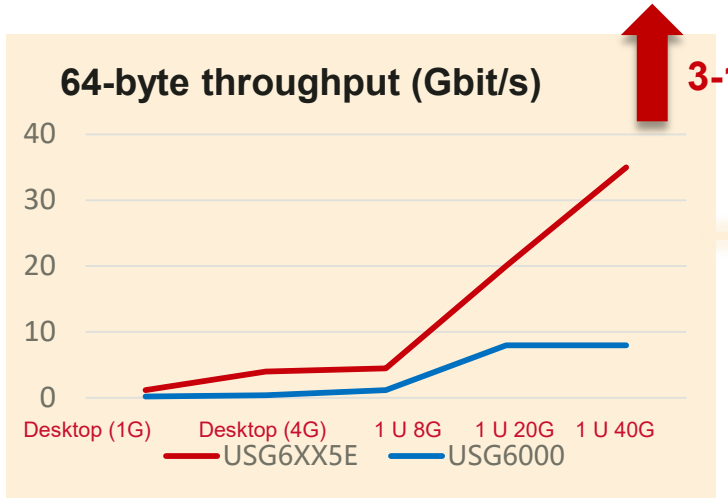
Flexible combination of hard disks

- Solid-state drive (SSD)/hard disk drive (HDD), stable and cost-effective

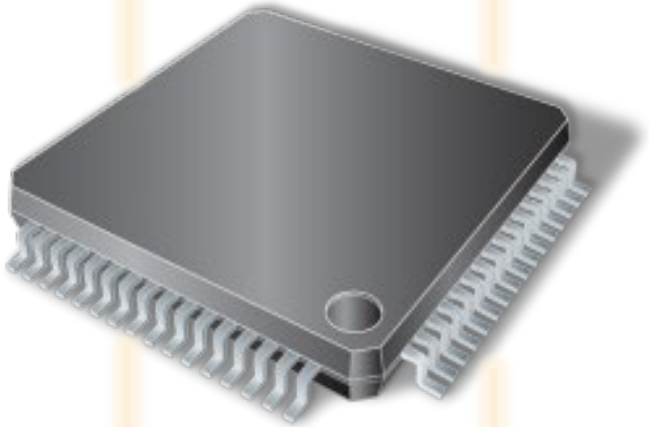
Diversified ports

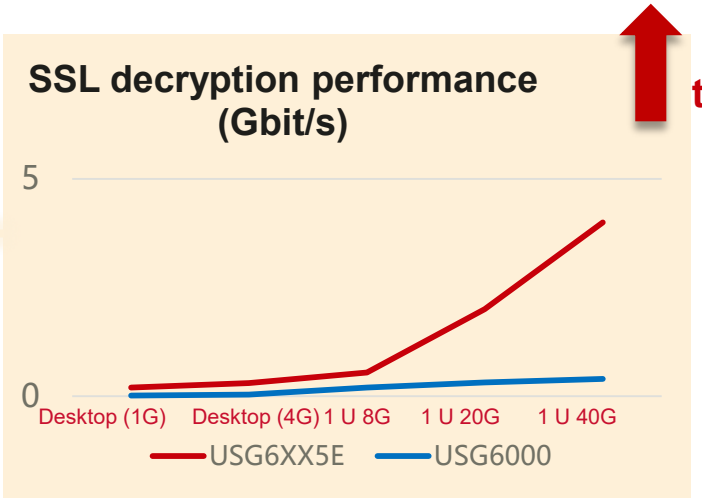
- GE/10GE/40GE ports
- 10GE/GE auto-sensing

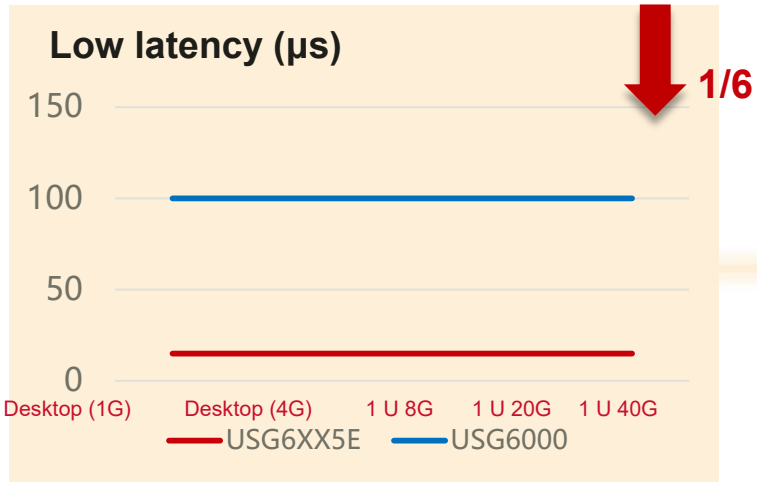
Huawei-Developed: Higher Performance Powered by Huawei-Developed Chipsets

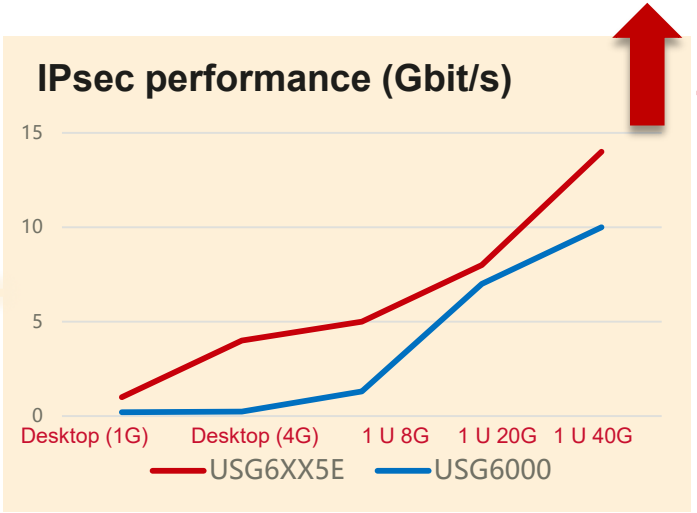


Huawei-developed chips greatly improve product performance.







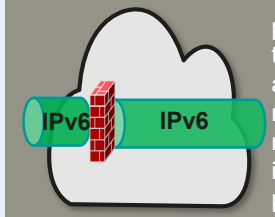


Network Expertise: Huawei's Secure and Abundant IPv6 Capabilities

IPv6 network switching

- IPv4/IPv6 dual stack
- DSLite tunnel
- NAT64 translation
- NAT66 translation

NAT66



Translates the public and private IPv6 addresses to reduce the difficulty in advertising the IPv6 routes of private networks and hide the internal IPv6 address to prevent external attacks.

IPv6 policy management and control

- Security policy
- Application control
- User management and control
- URL filtering

User authentication

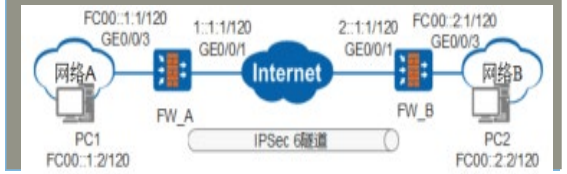
Identifies IP addresses of network traffic as users' IP addresses, provides user-based management for network behavior control and network permission assignment, and implements refined management.

IPv6 security protection

- Intrusion detection
- Antivirus
- Defense against attacks
- IPsec6

IPsec6

Improves communication security between IPv6 networks.

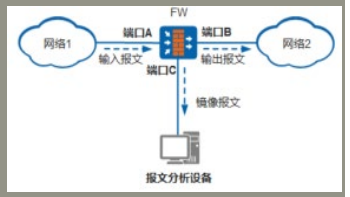


IPv6 service visibility

- Device management
- Traffic monitoring
- Application identification
- Logs and reports

Packet mirroring

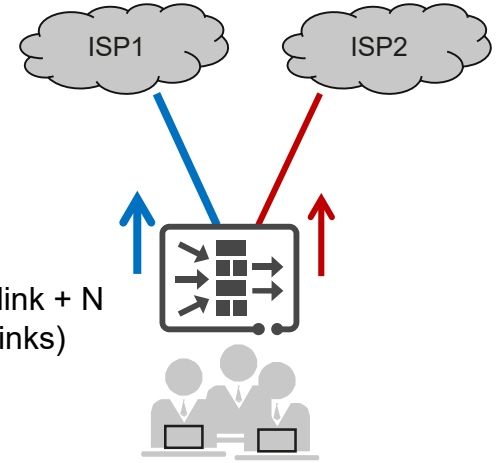
Obtains and analyzes session packets without interrupting services.



Network Expertise: Dynamic/Static Intelligent Uplink Selection Based on Multi-Egress Links

Static intelligent uplink selection

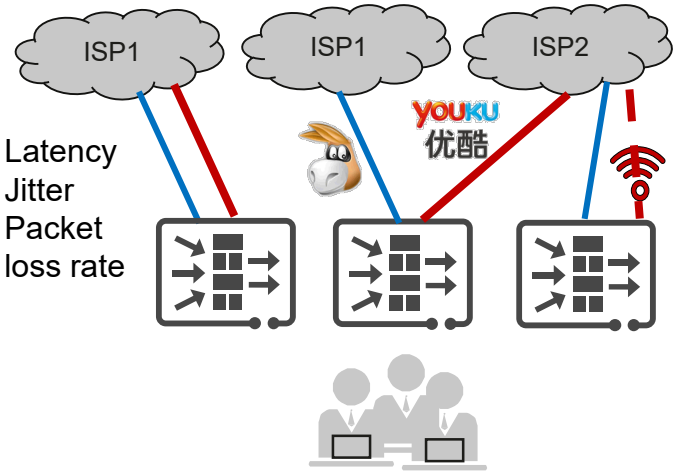
- Link weight
- Interface bandwidth
- Link priority (1 primary link + N secondary links)



- User-defined link weight
- Flexible traffic scheduling
- Flexible combination of multiple static intelligent uplink selection rules
- Uplink selection by binding ISP address sets to interfaces

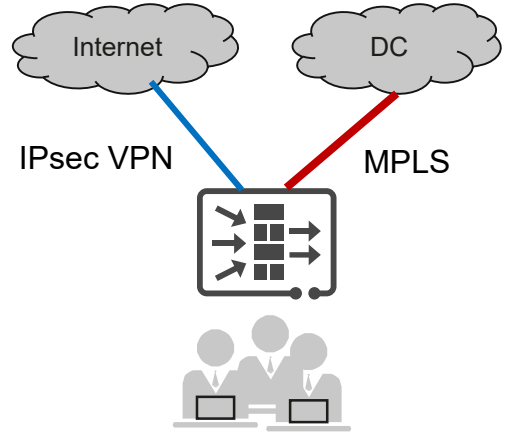
Dynamic intelligent uplink selection

- Latency
- Jitter
- Packet loss rate



- User-defined link SLA (latency, jitter, and packet loss rate), selecting the optimal link for traffic forwarding
- Application-based intelligent uplink selection
- Wired/wireless link switchover; wired link recovery, automatic wireless switching, minimum wireless link cost

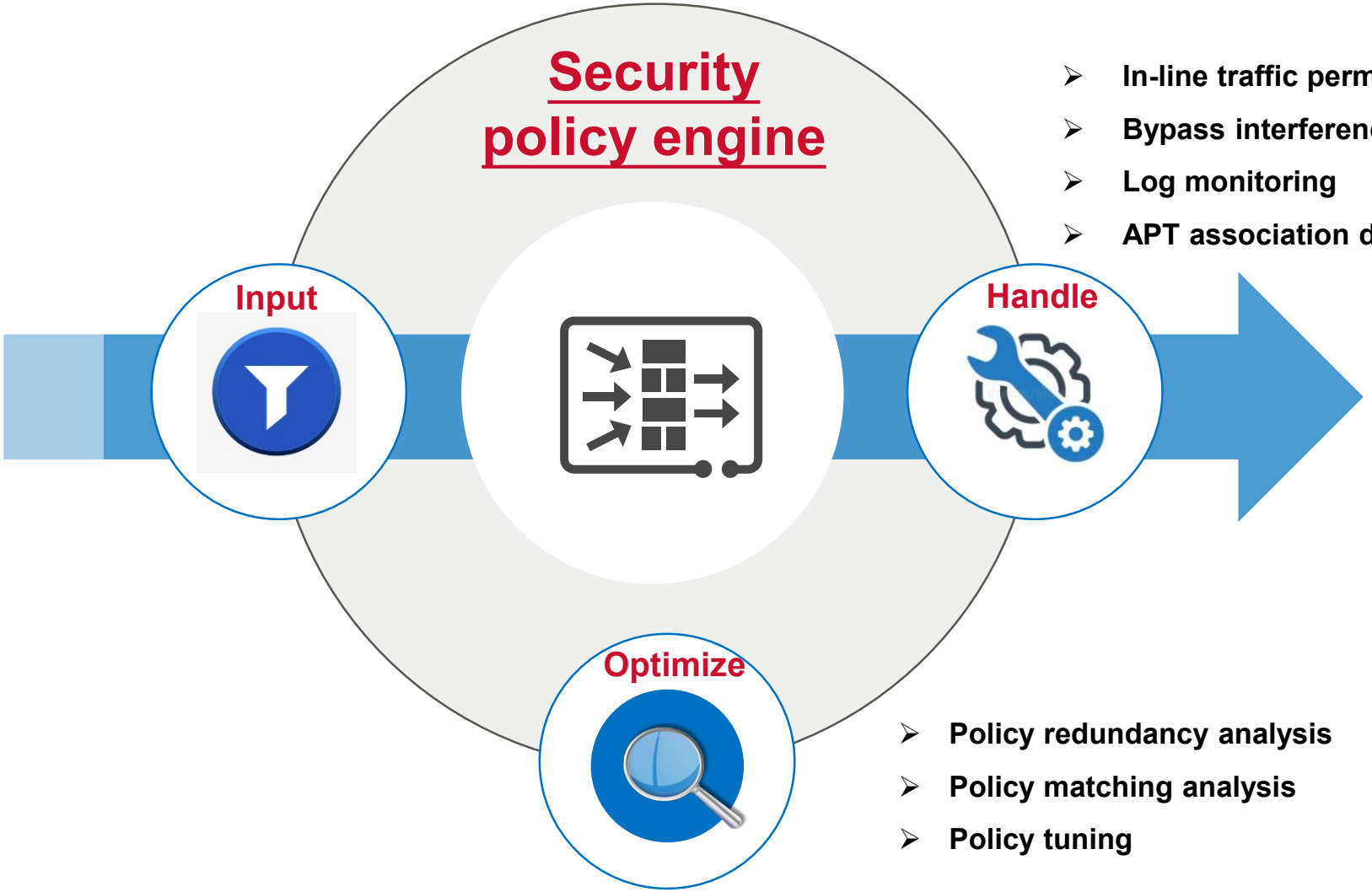
IPsec/Internet/MPLS-based uplink selection



- IPsec-based intelligent uplink selection
- Direct Internet access, private line uplink selection

Intelligent: Multi-Dimensional Awareness + Refined Control = Security Policy Control

- Quintuple traffic
- Service applications
- Access users
- URL information
- Geographical locations
- Threat information
- Time segment



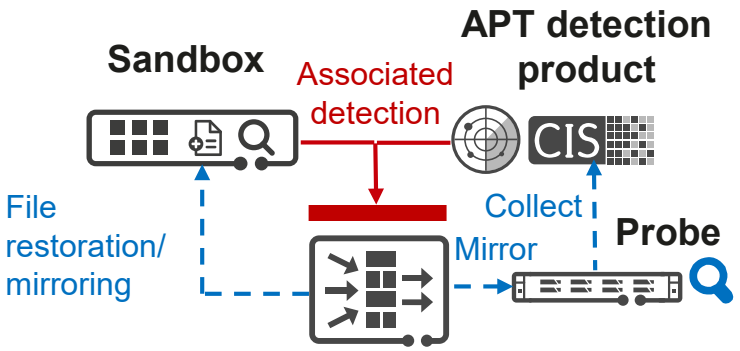
- In-line traffic permit/block
- Bypass interference packet
- Log monitoring
- APT association detection

- Policy redundancy analysis
- Policy matching analysis
- Policy tuning

Intelligent: Continuous Cultivation in Security Detection, Leading the AIFW Era

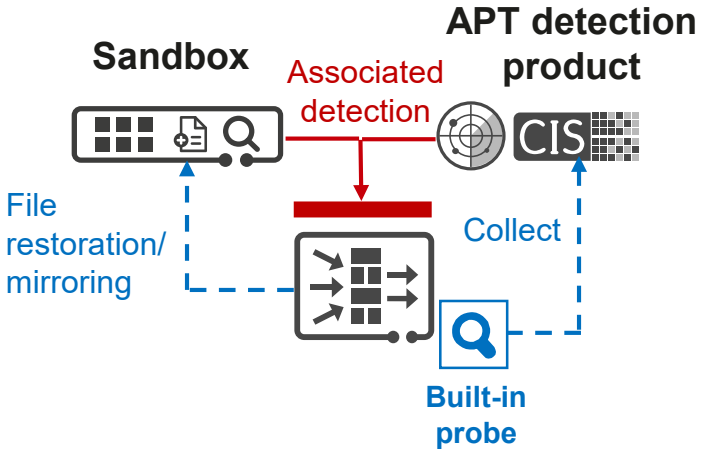
Most firewall vendors

Joint defense enforcement point



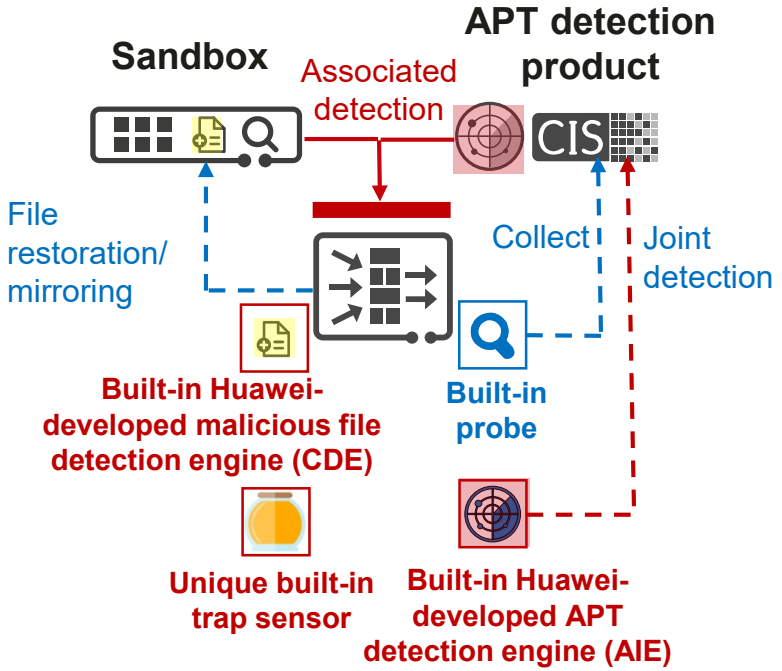
A few firewall vendors

Joint defense execution point + data collection point



Huawei AIFW

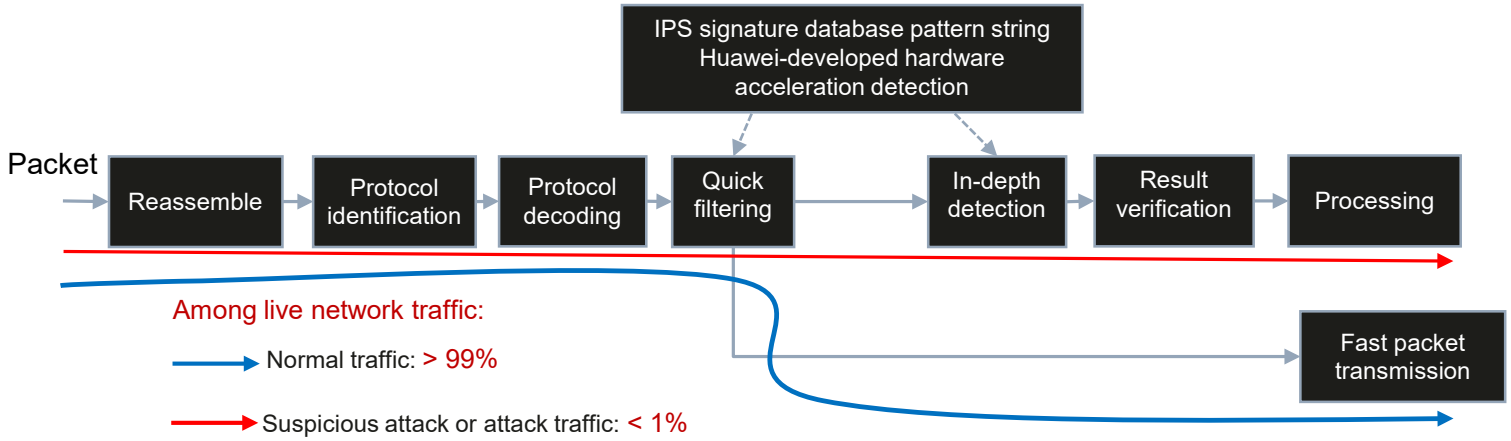
Joint defense execution point & data collection point + local APT defense point



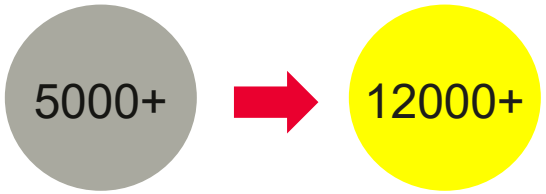
Intelligent: Comprehensively Improved IPS Inspection Capability

Intrusion Prevention System (IPS): Huawei-developed Multi-Dimension Detect Engine (MDDE), highlighted as follows:

- **Six key technologies**, ensuring inspection accuracy
- **Huawei-developed chip + pattern matching detection engine**, accelerating service processing
- **Refined pattern string state machine management**, increasing the number of rules that a signature database can accommodate
- **Compatible with the mainstream Snort syntax**, customizing and configuring many more threat detection rules in a more flexible manner

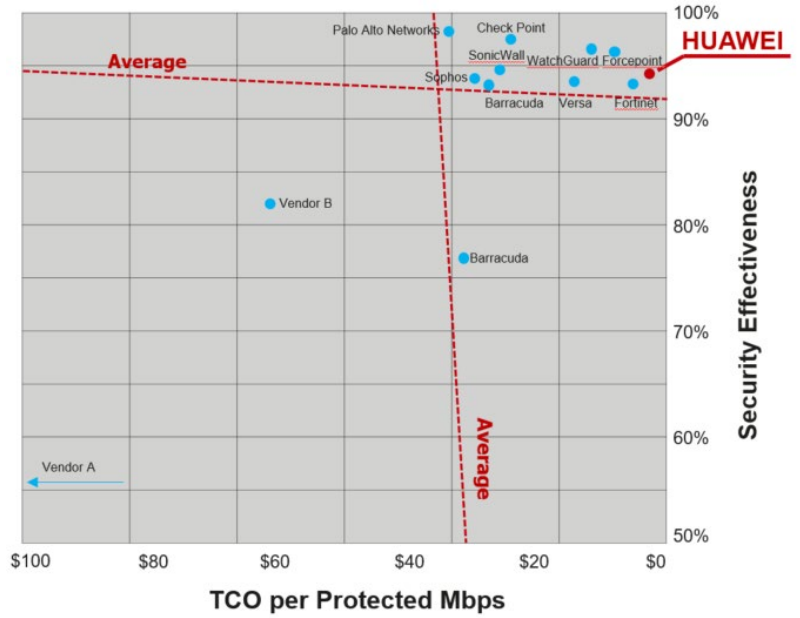


1	2	3	4	5	6
Out-of-order packet reassembly detection	Protocol identification for all traffic	Refined decoding for post-identification traffic	Protocol anti-evasion detection	Protocol classification + patten matching	Quick filtering of unidentified traffic + in-depth detection



2x↑ defense signatures, with stable defense performance

"Recommended" rating in NSS Labs 2019 NGFW Group Test

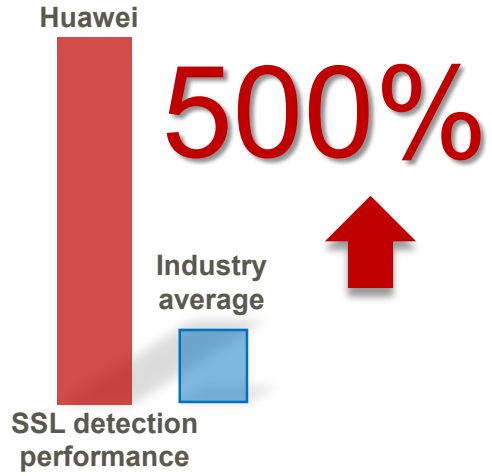


Intelligent: Continuously Optimizing the OpenSSL Library, 5X↑ Performance

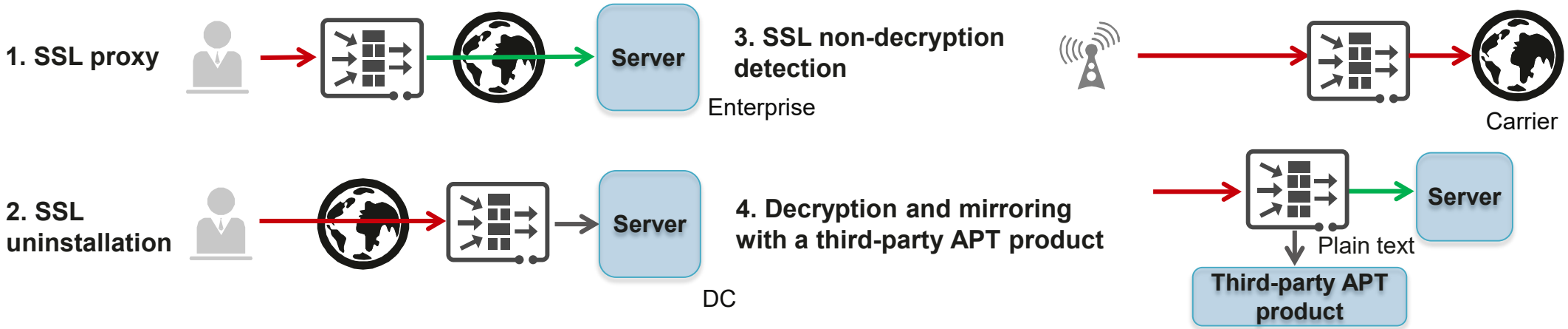
Continuous Transport Layer Security (TLS) tracking
Huawei is an important player in the IETF standard organization and can quickly support the latest TLS protocol version.

OpenSSL library optimization
Develop a dedicated OpenSSL library interface, **doubling** the process efficiency.

Chip hardware acceleration
Continuously track the application of the latest algorithms (such as X25519).
In the industry, only Huawei's next-generation acceleration chips can implement acceleration for this algorithm



Abundant SSL detection capabilities



In the latest version, TLS1.3 can perform SSL proxy and SSL uninstallation over encrypted traffic.

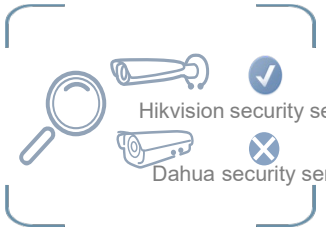
Intelligent: Trustable, Controllable, Secure Terminal Access, Network-Wide Theat Visualization

Block Unauthorized Terminals

First security line: access authentication (easy-to-deploy)

To be applicable to other IoT devices

Block Unauthorized Services



Second security line: in-depth anti-spoofing, intrusion prevention

Block Malicious Traffic

Third security line: ever-updating security capabilities

1 Device fingerprint-based authentication

- Dynamically collect camera fingerprints
- Generate authentication factors based on fingerprints
- Proactive detection, dynamic evaluation
- Implement unique fingerprint authentication

2 Traffic fingerprint-based filtering

- Dynamically detect security service traffic, generate traffic fingerprints
- Perform access control based on traffic fingerprints

3 Protocol-based vulnerability defense

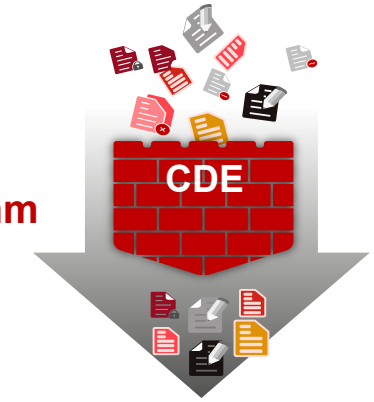
- Focus on camera vulnerabilities to form a vulnerability signature database, preventing attackers from breaking down cameras on a large scale by exploiting camera vulnerabilities
- Update the IPS vulnerability database in real time

Comprehensive asset management platform (Border Eyes)

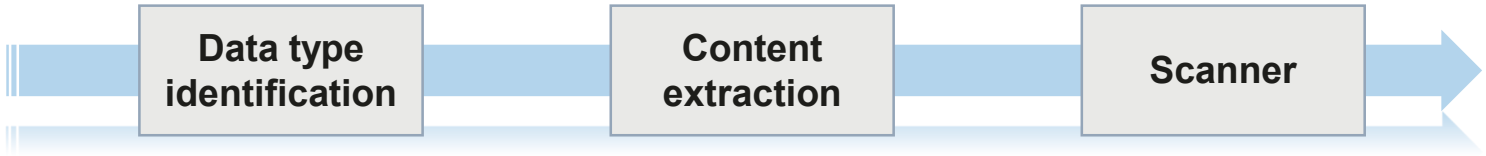
Asset management, attack defense, configuration management, service statistics collection, log management, one-screen monitoring

Intelligent: Huawei-Developed Malicious File Detection Engine + IPS

- Two-year R&D
- PA Class 2.0 AI algorithm



- Redefine malicious file detection using AI

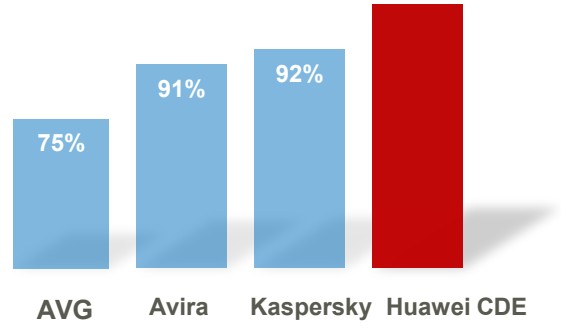


- PE files (exe, .dll)
- Script files (Javascrpit)
- Composite documents
- HTML files
- Compressed files (.tar, .7zip, .zip)

- Dejacketer
- Script standardization
- Composite document analysis (VBS/JS/sub-PE)
- HTML extraction (script/IFrame)
- Depacketizer

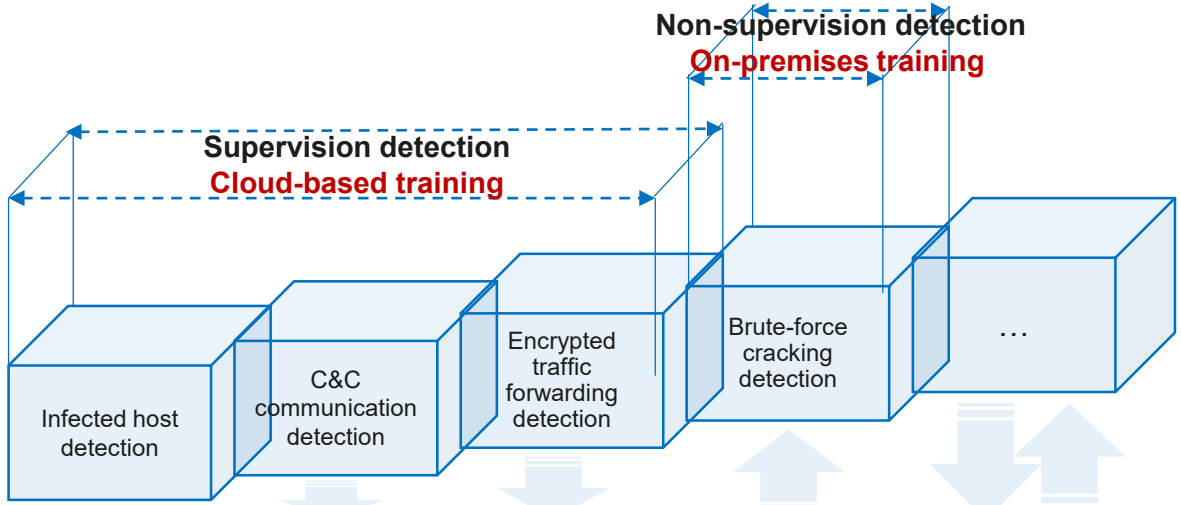
- Multimode scanner
- Hash scanner
- Heuristic scanner
- AI scanner

Malicious file detection rate **97%**



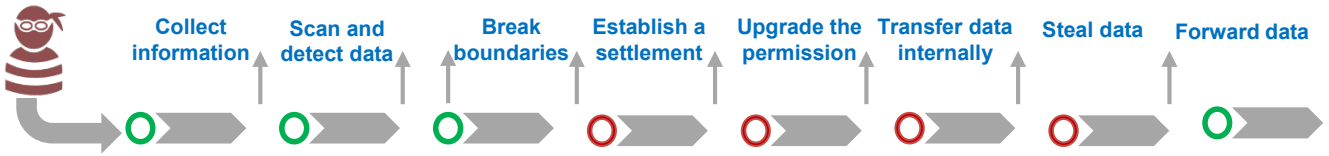
Test time: average detection rate in 30 days, March 2019
Test method: 500,000 VirusTotal samples per day

Intelligent: Unique AIE APT Defense Engine, Continuously Defending Against the Latest Threats



- The cloud delivers the latest threat detection models to customers. Customers are free from version update.
- Huawei continues R&D in AI APT detection to cope with more threats.

20+ patents

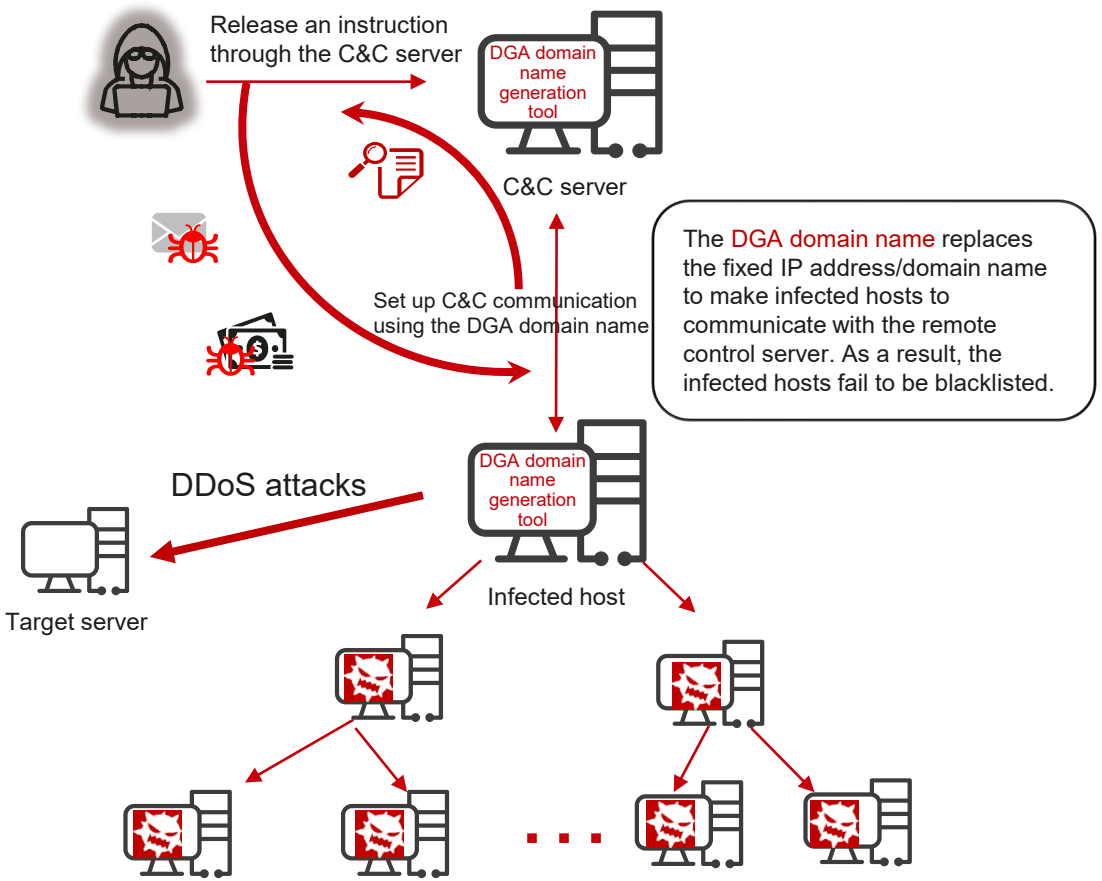


Customer Benefits

- Discover **more threats** with **less costs**, achieving **"inclusive AI"**.
- **Local APT detection**, **50%+** faster threat response than cloud-based detection
- **Latest threat defense capabilities from the cloud** to customers, free customers from version update
- Comprehensive network risk evaluation, defense against network threats on the attack chain

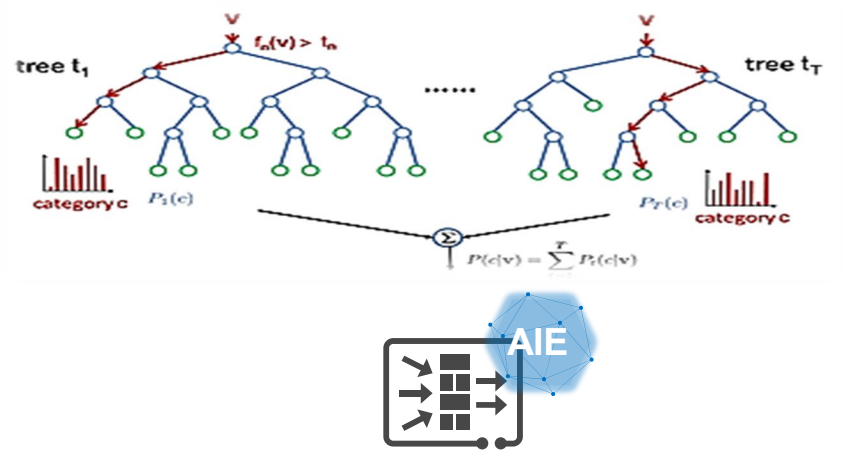
Intelligent: AI-Powered Detection of Infected Hosts, Detecting 99% DGA Domain Names

30% of malicious domain names are DGA domain names



1 million+ black samples

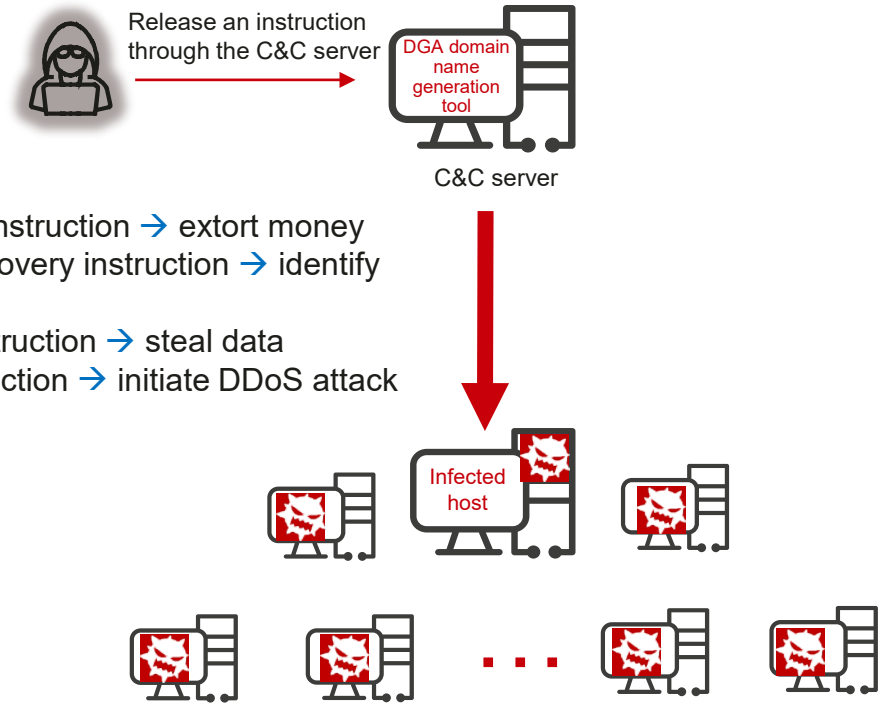
50 sample families



99% DGA domain name detection rate

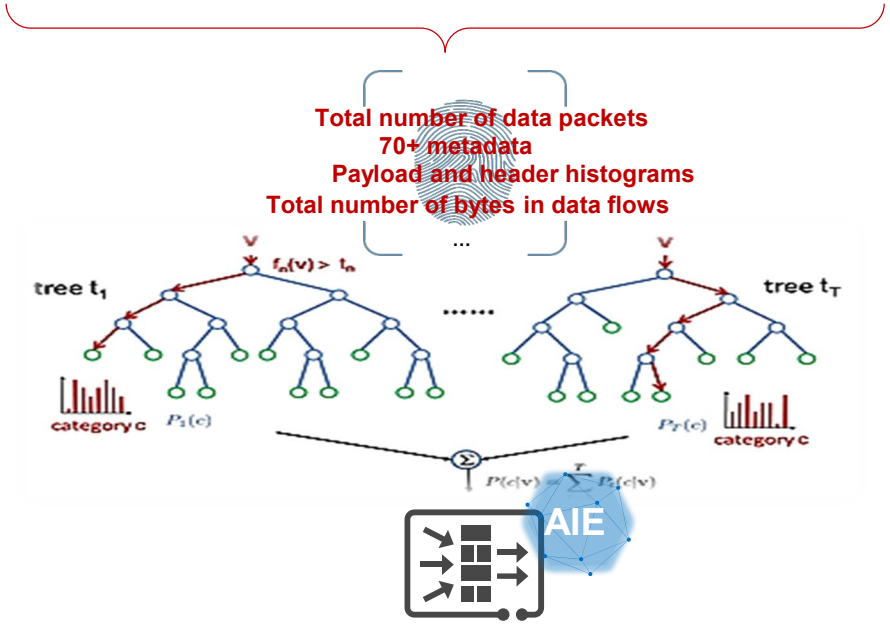
Intelligent: AI-Powered C&C Detection, Efficiently Blocking APTs

C&C is a necessary action for hackers to deliver attack instructions. If C&C can be identified, the attack source and zombies can be accurately identified.



- Encryption instruction → extort money
- Internal discovery instruction → identify key assets
- External instruction → steal data
- Attack instruction → initiate DDoS attack

90,000+ black samples **39** sample families

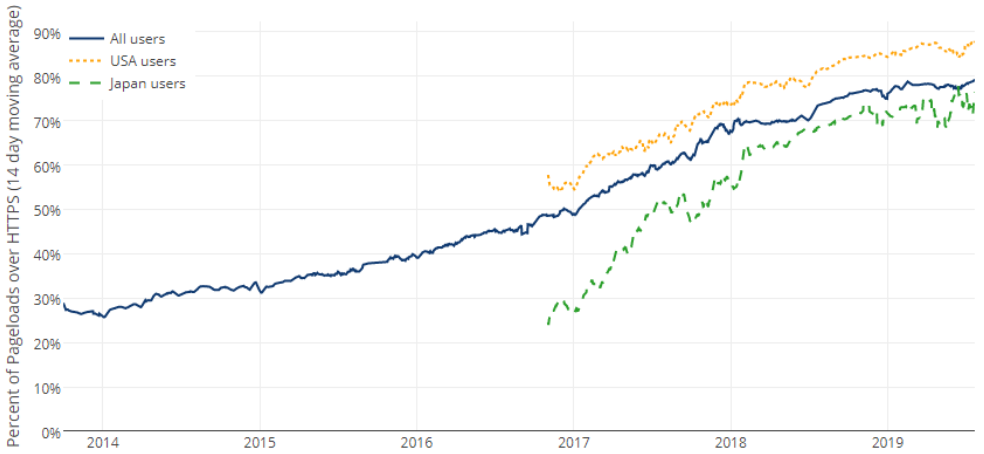


98% C&C detection rate

Intelligent: AI-based Decryption-Exempted Traffic Detection

70%+ encrypted traffic

30% threat traffic



Source: Firefox telemetry, 14-day moving average

Top 254 enterprises, with an average annual loss of **US$5 million** each enterprise

Admin US
Partners
VirusTotal

2.5 million+/day

White samples

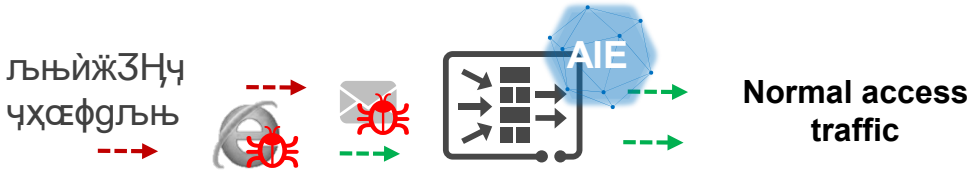
Open samples
Huawei cloud sandbox
Partners/Colleges and Universities

40,000+/day

Black samples

TCP traffic statistics characteristics
TLS handshake information characteristics
Associated DNS information characteristics
Associated HTTP information characteristics
...

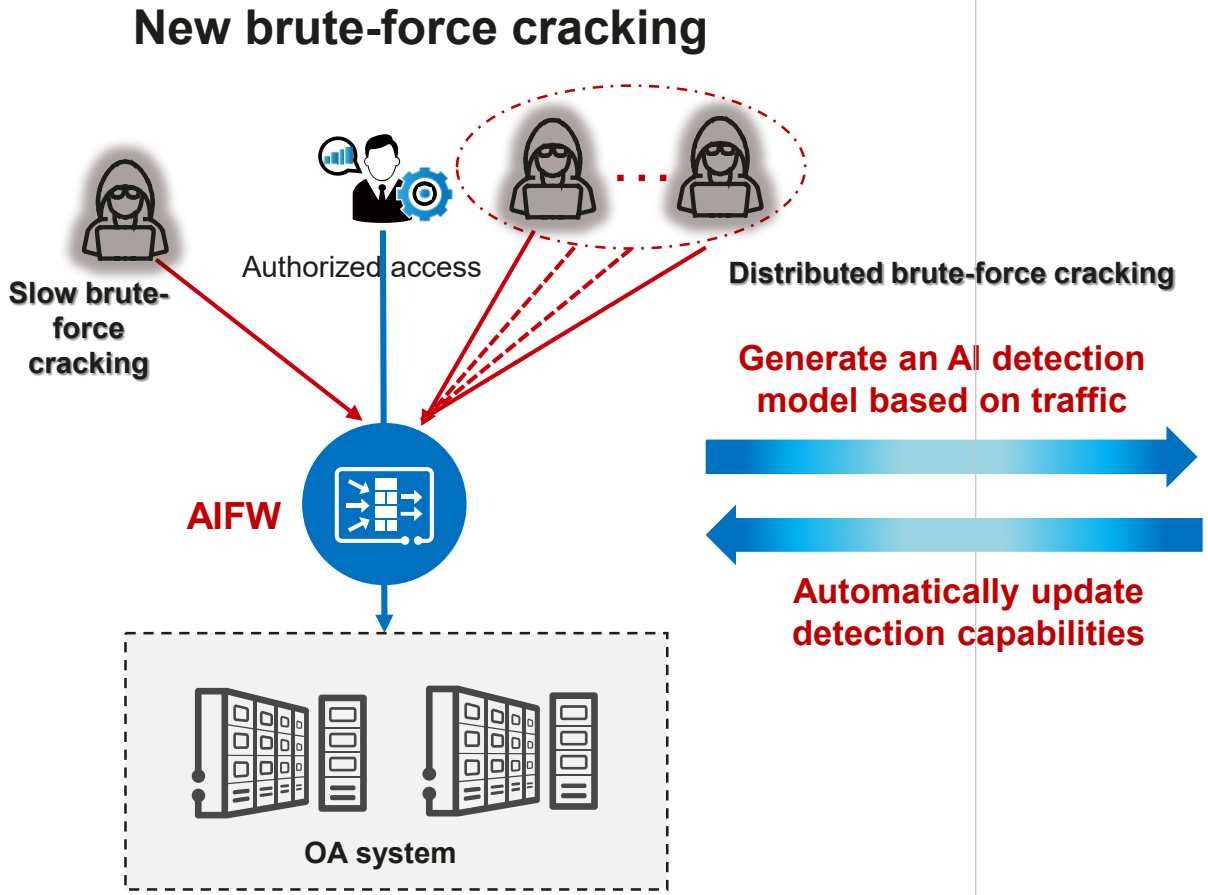
200+ detection characteristics



500+ encrypted communication sessions detected on a single day at a site

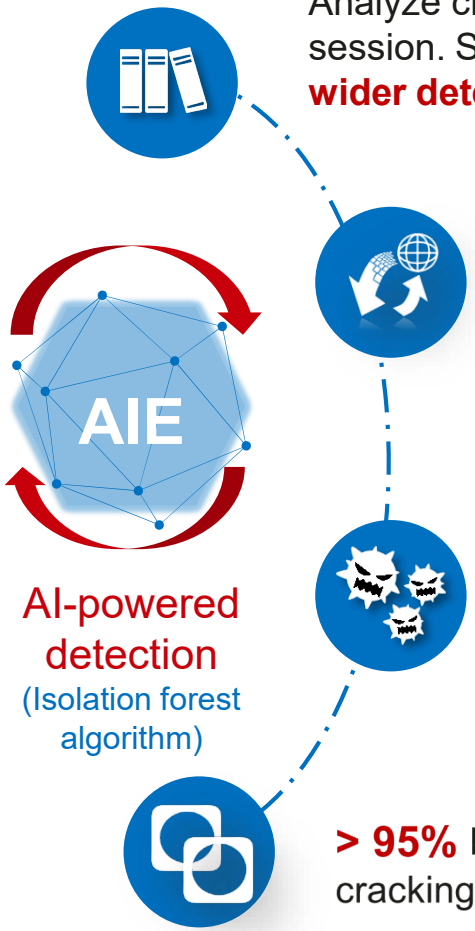
99% detection rate

Intelligent: AI-Powered Detection Model, Identifying Threats More Accurately



Generate an AI detection model based on traffic

Automatically update detection capabilities



Analyze characteristics of a single session. Support **more protocols** and **wider detection scope**.

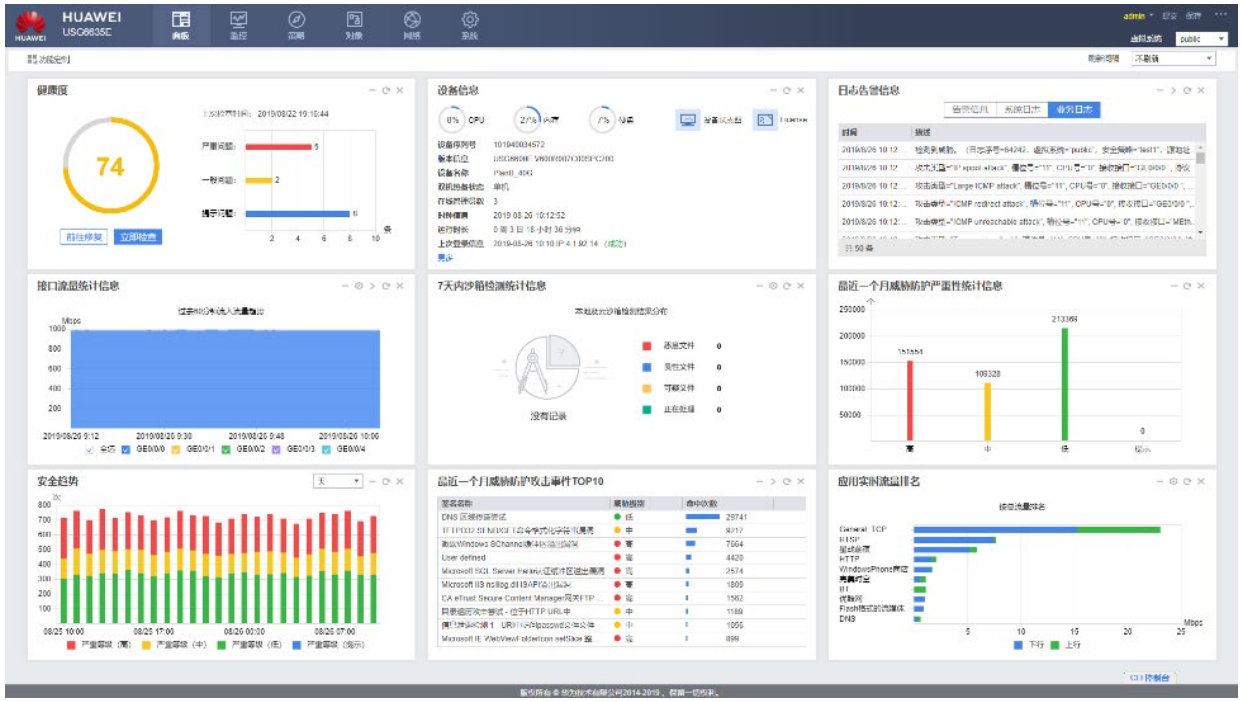
Use the AI detection algorithm to effectively identify brute-force cracking on the **intranet and extranet**.

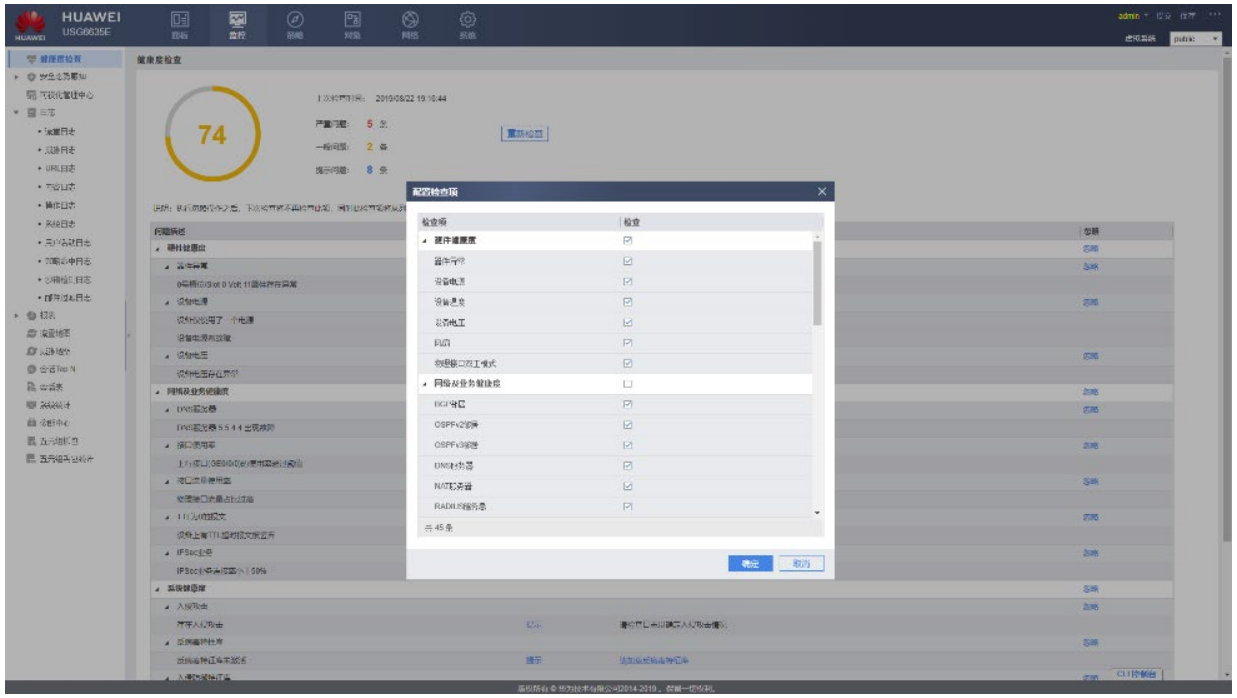
Detect **distributed** brute-force cracking based on the IP association algorithm.

> 95% brute-force cracking detection rate

Simplified: Unremitting Commitment to Easy-of-Use, Reaping Brand-New Web UI 2.0

Redefine the UI based on threat visualization



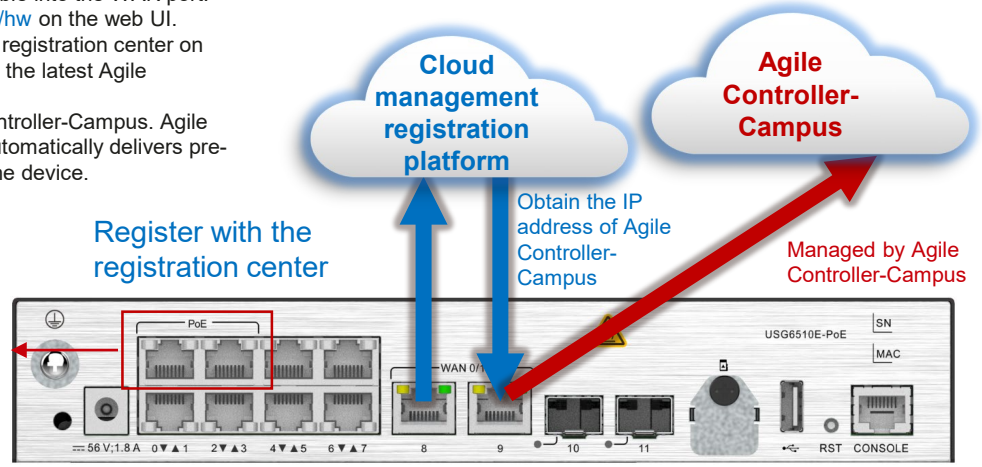


Simplified: Multi-Branch Cloud Management Oriented at Easy-of-Use

A device gets managed by Agile Controller-Campus in three steps:

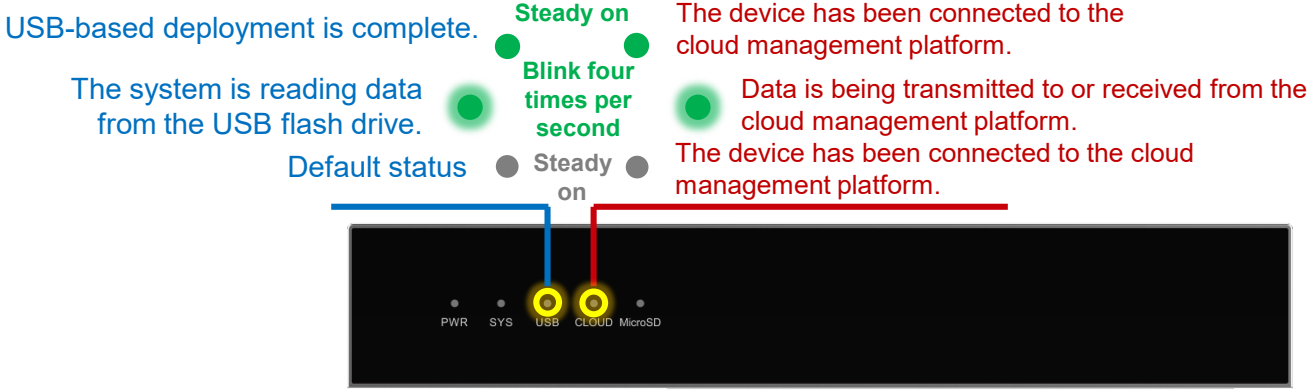
1. Obtain an IP address.
   DHCP: Insert a network cable into the WAN port.
   PPPoE: Enter 192.168.0.1/hw on the web UI.
2. Get connected to the DNS registration center on HUAWEI CLOUD to obtain the latest Agile Controller-Campus.
3. Get connected to Agile Controller-Campus. Agile Controller-Campus then automatically delivers pre-defined configurations to the device.

Zero Touch Provisioning (ZTP)

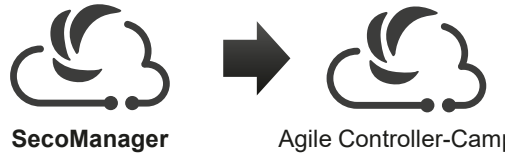


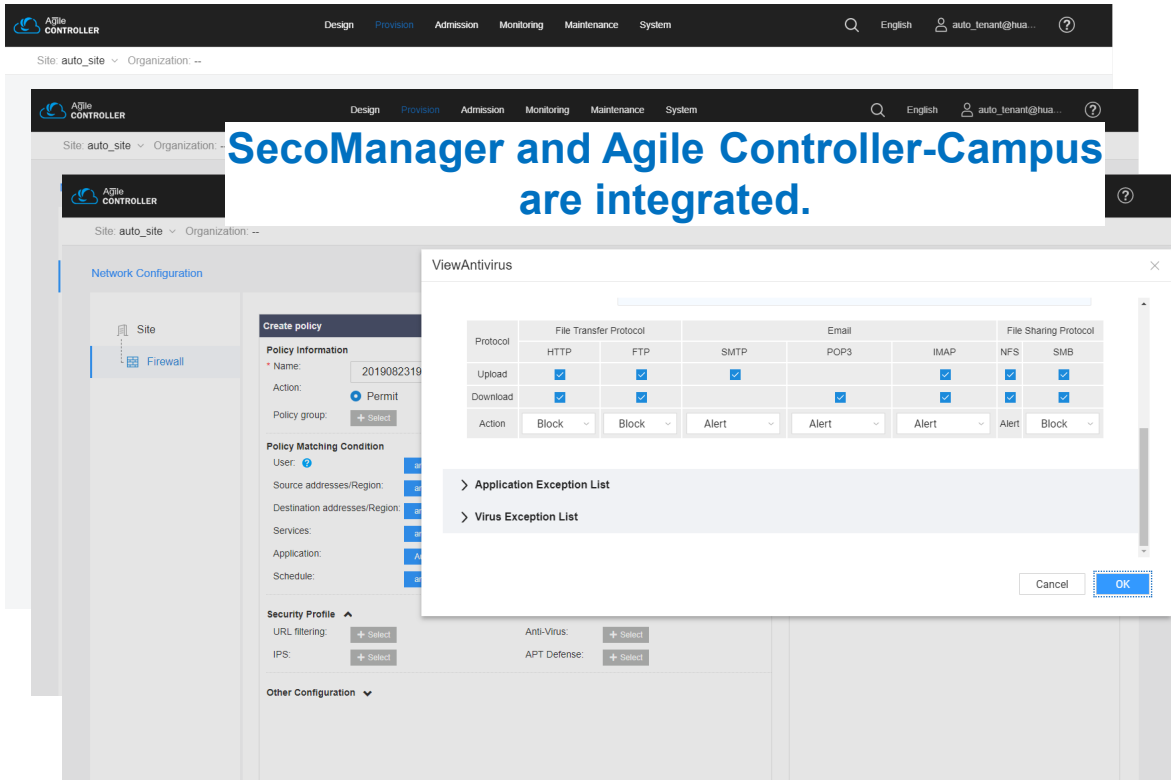
2 PoE+ or 4 PoE ports, applicable to small-branch power supply

Ease-of-use hardware



SecoManager is integrated into Agile Controller-Campus as an app.



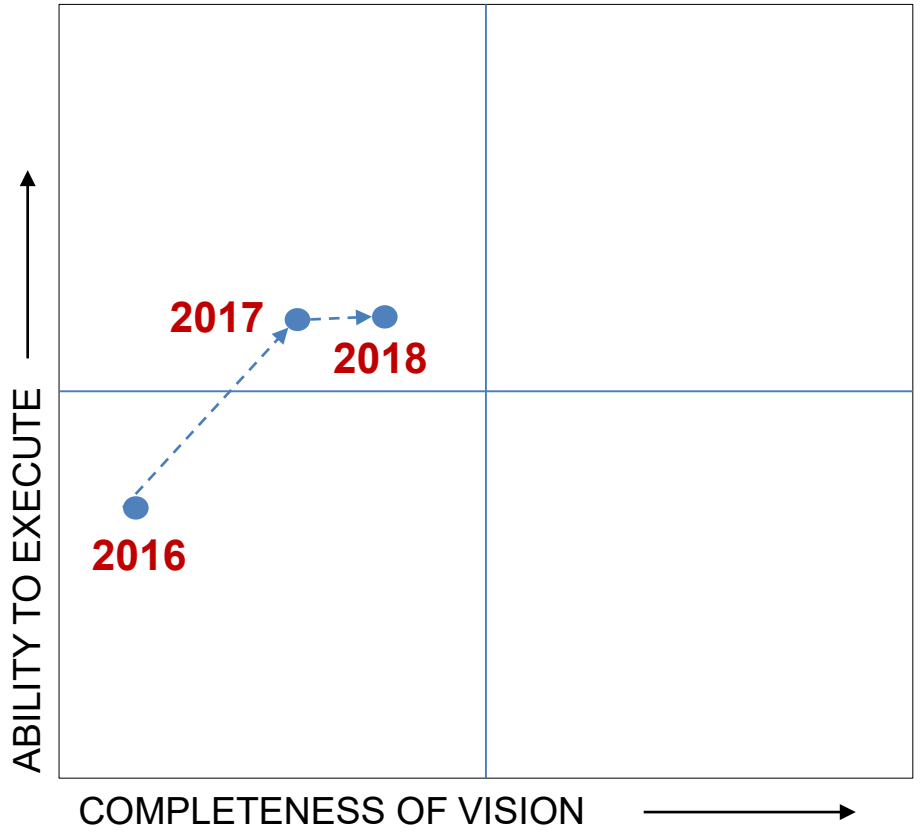


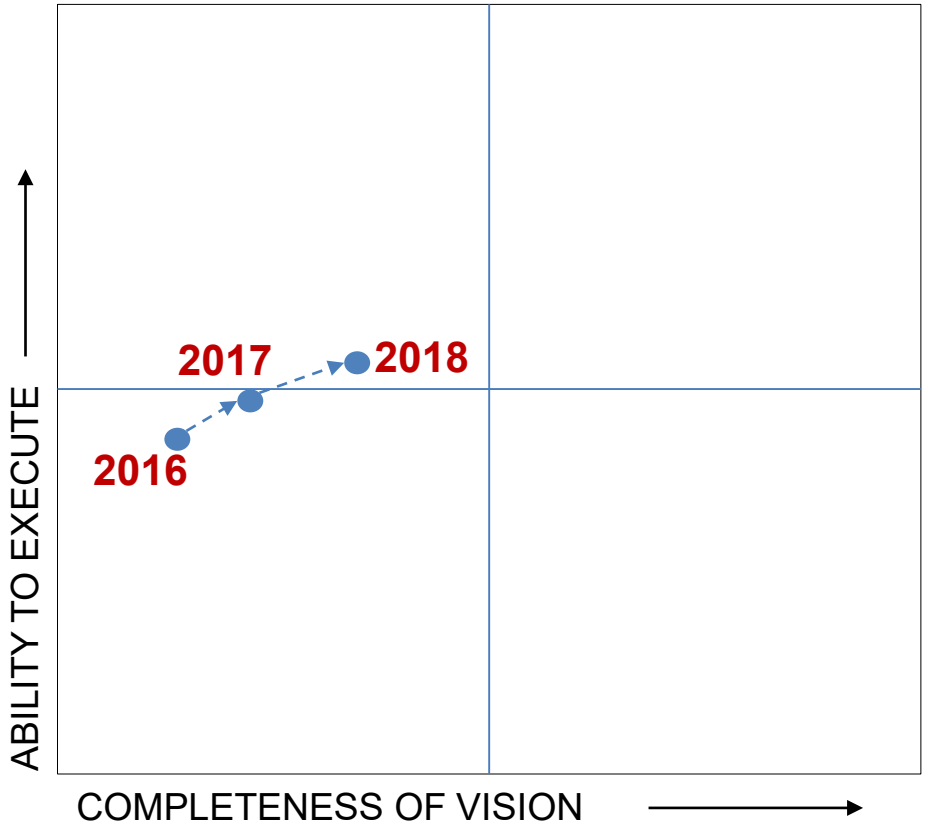
Configure and manage advanced security services, such as IPS, antivirus, URL filtering, and anti-APT

Contents

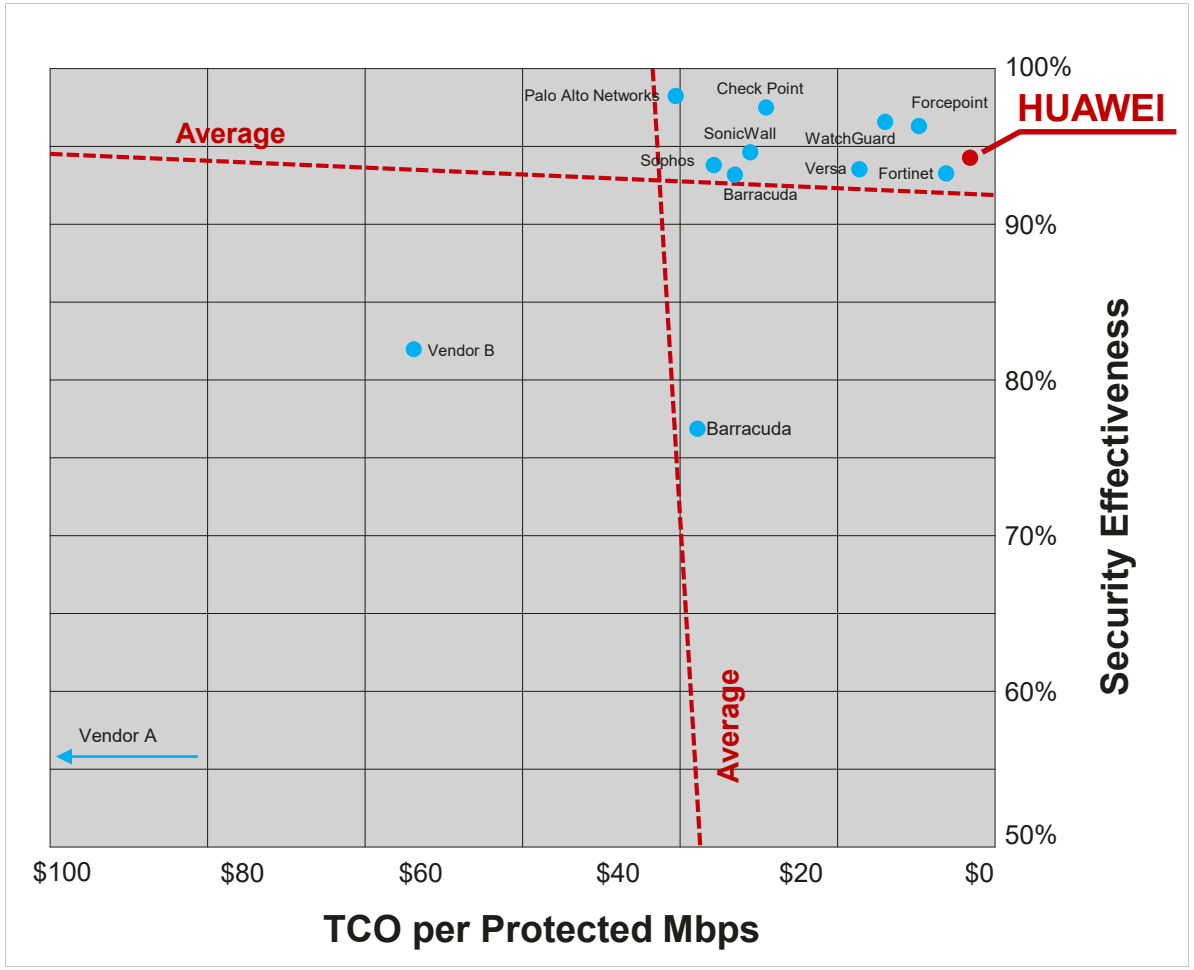
Huawei NGFW, Unremittingly Committing to Better Security Defense Capabilities

Huawei was positioned as a "Challenger" in Gartner 2018 Magic Quadrant for NGFW and UTM.





Huawei NGFW Earned a "Recommended" Rating in NSS Labs 2019 NGFW Group Test



Hard core security, unique in China, recommended again

Highlights of NSS Labs 2019 NGFW Group Test:

- 12 NGFWs from industry-leading security vendors
- Only NGFWs with top technologies and competitiveness are eligible for the "Recommended" rating.

Why does Huawei NGFW earn a "Recommended" rating **again**?

- USG6620E earned the top "Recommended" rating for its outstanding performance in threat blocking rate, threat anti-evasion, stability, and reliability.
- Highest cost-effectiveness of Huawei NGFW in the industry for its much lower total cost of ownership (TCO) per Mbps than most of those from other participating vendors

Contents

Success Story (1): Jingdong

Core competitiveness: rapid logistics service

Over 35 million
commodities per day

Huawei firewalls help Jingdong build an efficient and secure logistics system. Logistics information is quickly and securely transmitted between Jingdong headquarters and thousands of remote branches. The rapid logistics service has become the core competitiveness of Jingdong.

JD.com

Success Story (2): ICBC

Annual online transaction quantity:

> 380 trillion

Online transaction quantity:

47 billion

Individual users:

> 393 million

Huawei helps Industrial and Commercial Bank of China (ICBC) build an all-round security architecture through secure data center transmission, security management, virtualized security operation, and production/data network isolation so that ICBC manages and controls information security risks in an efficient manner.

中国工商银行
INDUSTRIAL AND COMMERCIAL BANK OF CHINA

Success Story (3): Schools in CLM of Spain

Huawei Firewall Pros:

- Provides network security protection for school networks, including intrusion prevention, antivirus, and encrypted web security check.
- Prevents primary and secondary school students from accessing illegal websites containing pornography, gambling, or drugs.
- Performs application control and bandwidth management based on users, time segment, and applications.
- Performs IPsec-based interconnection with non-Huawei firewalls.

725 schools

In Castilla-La Mancha of Spain, Huawei deploys high-speed Wi-Fi networks for primary and secondary schools, enabling teachers and students to access the Internet in a fast and secure manner, and securing connection channels between data centers of education networks. This project uses Huawei future-proof CloudCampus solution involving Wi-Fi, switches, and firewalls.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI