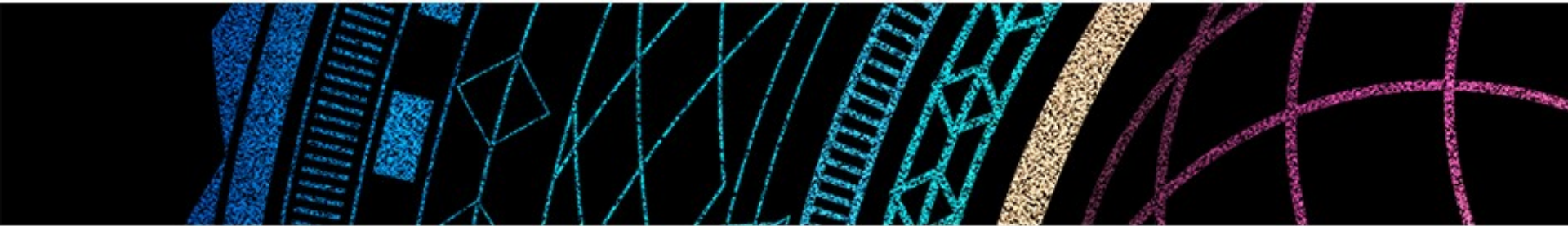


# Big Data Enhances Huawei Security Products and Solutions

Liu Lizhu, Vice President of Huawei Enterprise Networking  
Product Line

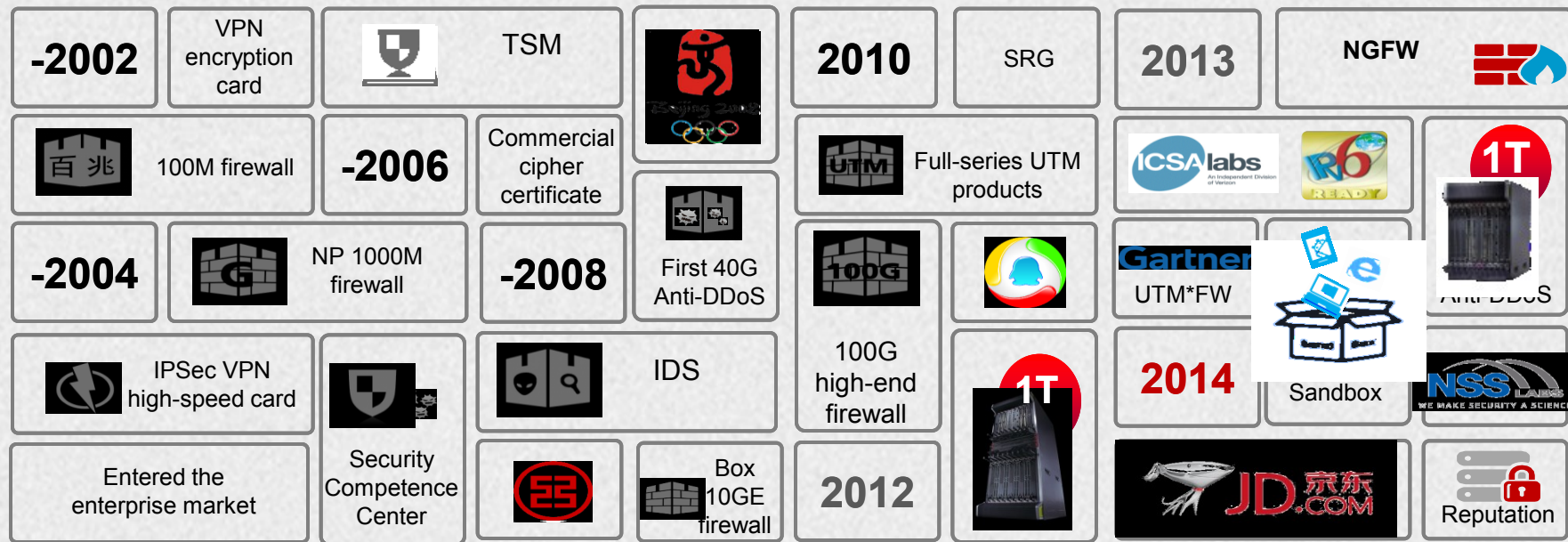


敏捷已来

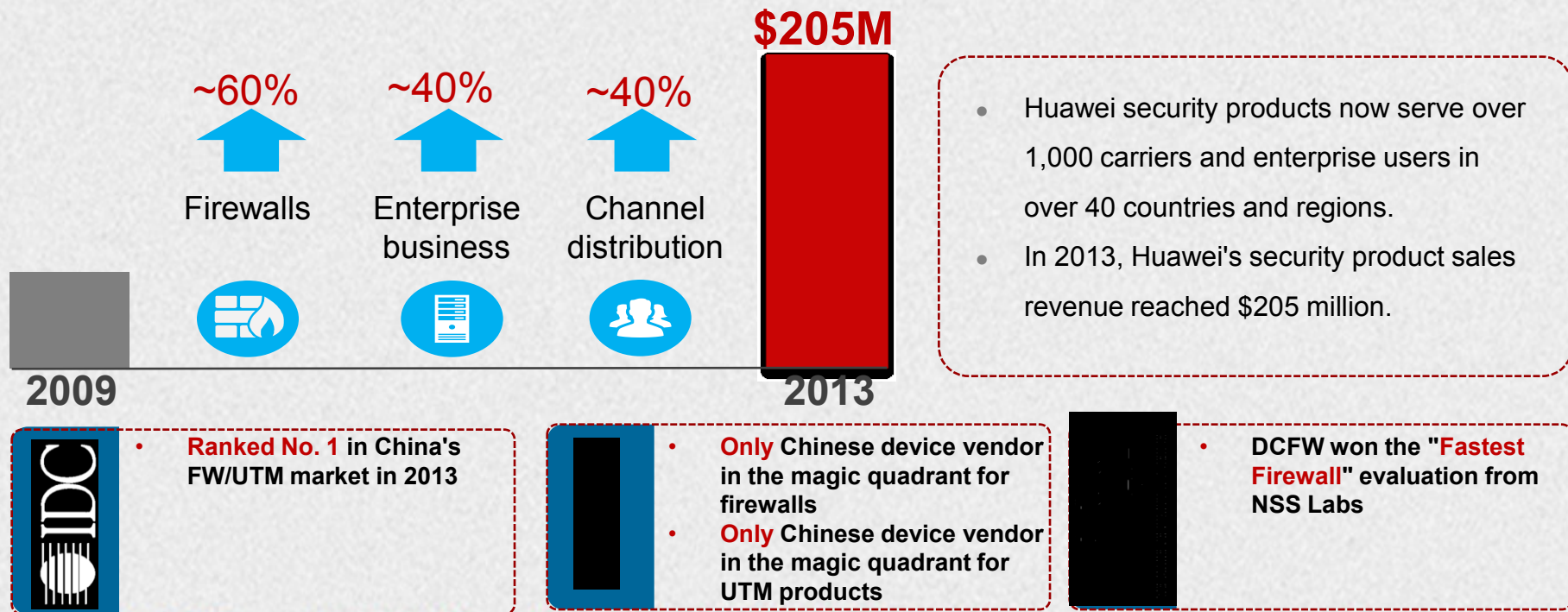
**Weaving The Future**

*Envision A Better Connected World*

# Ten Years of Rich Experience in the Security Field

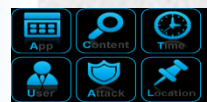
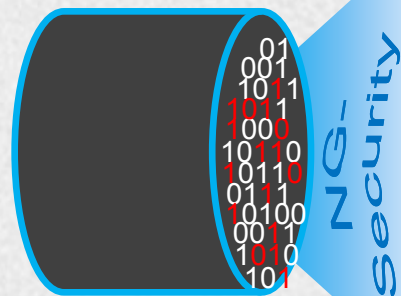


# Huawei's Security Business in 2013





# Huawei Next-Generation Network Security



Awareness



Analysis



Automation

## Intelligent Management & Control:

- 6-dimensional awareness
- Policy auto-optimization



Data Collection



Data Analysis



United Security

## United Security:

- Big Data analytics
- Device collaboration over the entire network



Application Identification



7-Layer Protection



Topspeed Experience

## High Efficiency and Accuracy:

- T-level performance
- Identification of 6,000+ types of applications

# What Is Big Data Analytics?

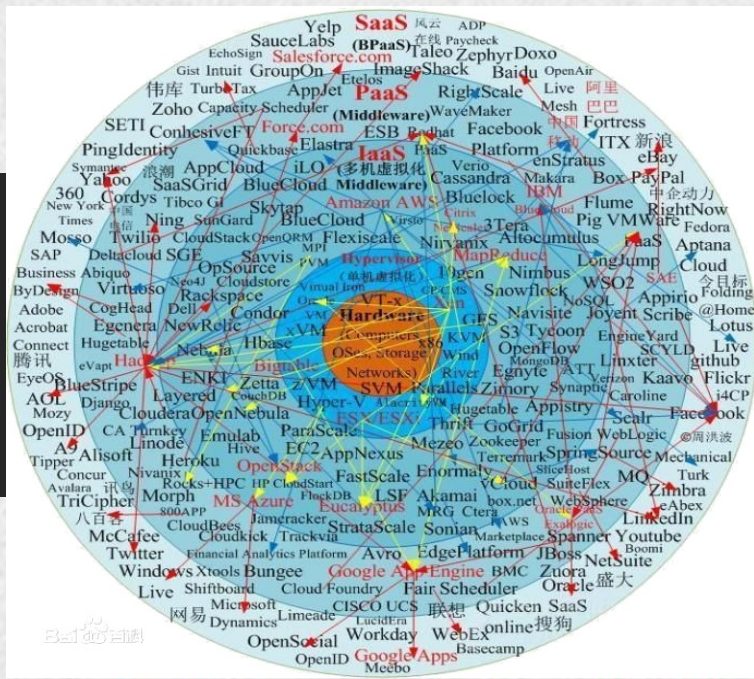
## ■ "4V" characteristics of Big Data:

- **Volume:** large volumes of data
- **Velocity:** high processing speed
- **Variety:** various types of data
- **Value:** low value density and high commercial value

Big Data analytics means performing analytics of large-scale data with the "4V" characteristics and generating high-value results.

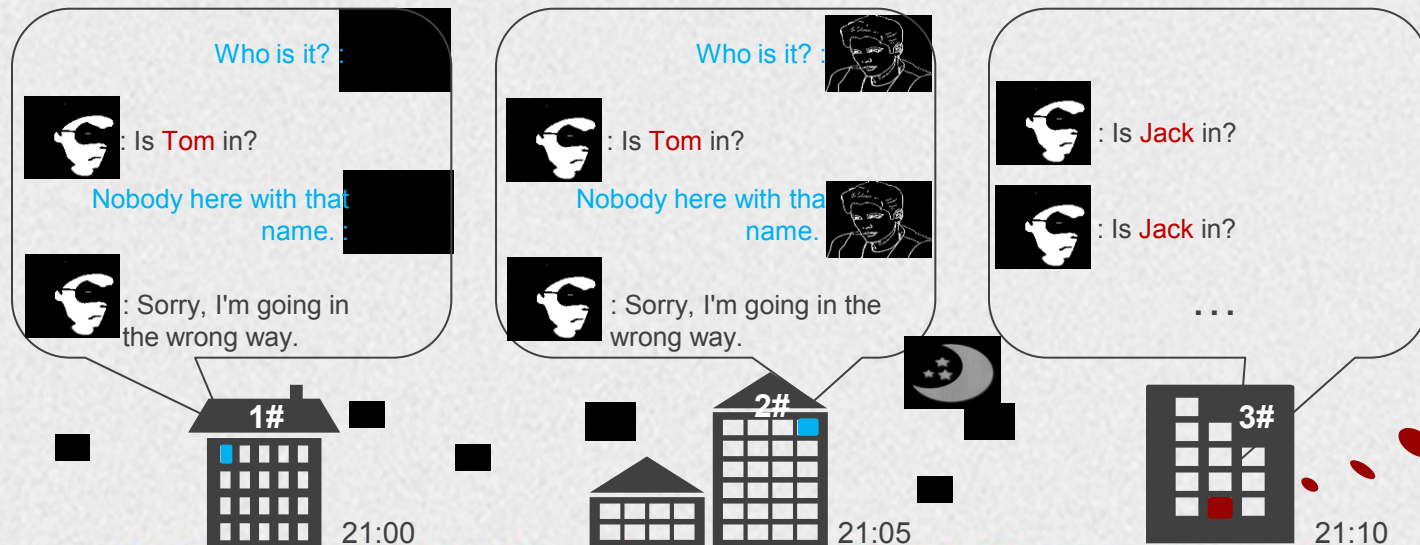
## ■ For example:

- Google accurately forecasted occurrence and spreading of the first influenza in the U.S. using Big Data analytics based on hot search words such as symptom and medicine.



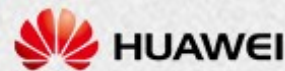
# How to Apply Big Data Analytics to Network Security?

When there was a knock on the door...

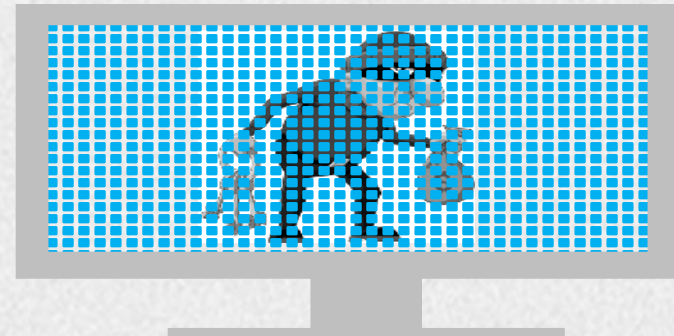




# Big Data Analytics-based Threat Defense in a Smart Residential Community



- **Collection:** Cameras collect all door-knocking behaviors.
- **Analytics:** Campus control center performs Big Data analytics.
- **Display:** Obtains abnormal behaviors through analytics.
- **Response:** Sends an "abnormal behavior" alarm.



Threat prevention is implemented based on Big Data analytics.



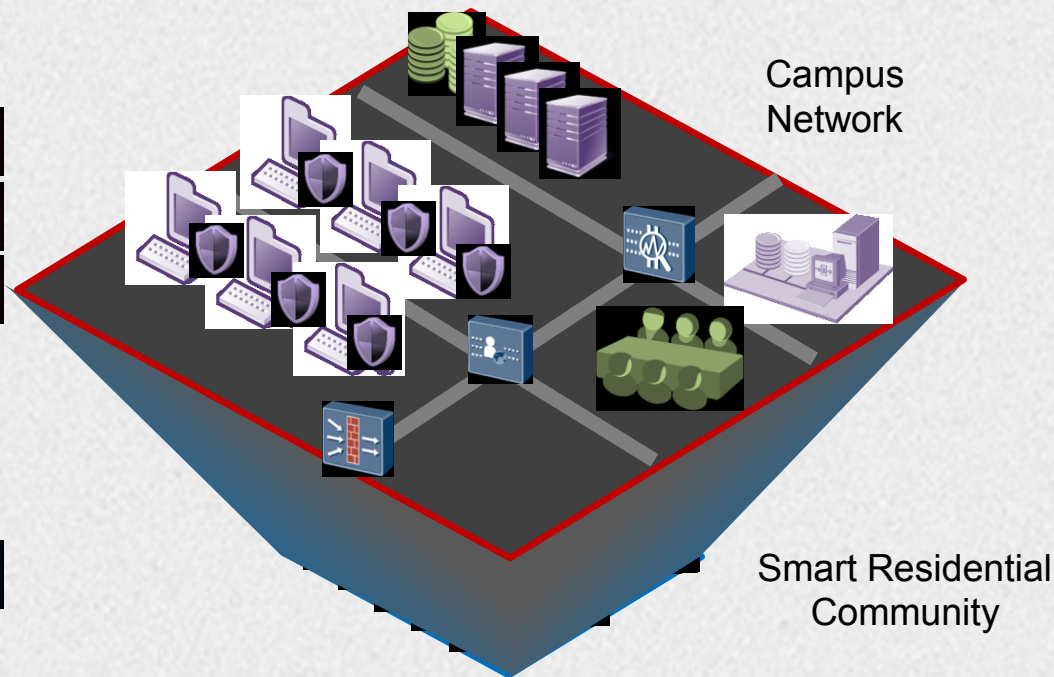
# Enterprise Campus Networks Also Exist the Same Risk

## Environment Is Changing

- Vague security defense border
- Various attack means
- Threats from known to unknown

## Changeless Protection

- Decentralized deployment and single-point defense
- Lack of collaboration and global inspection
- Fail to predict potential threats





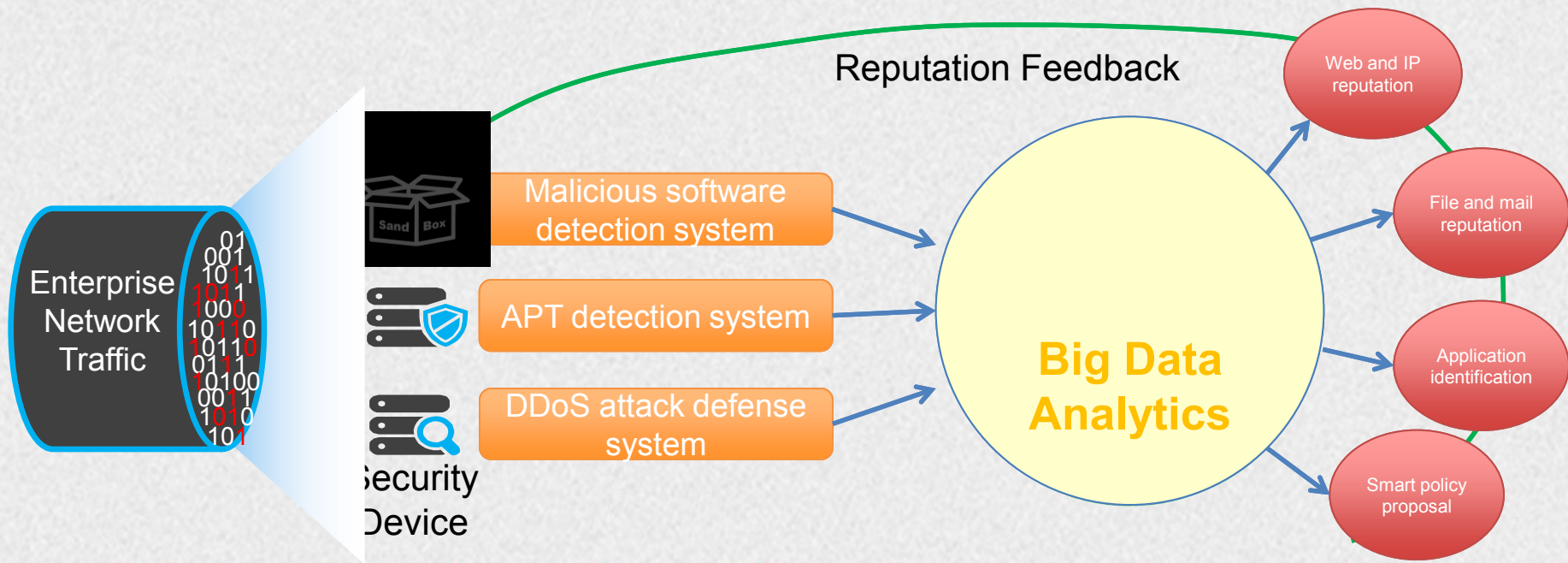
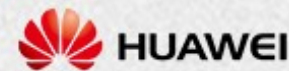
# Security Intelligence Center



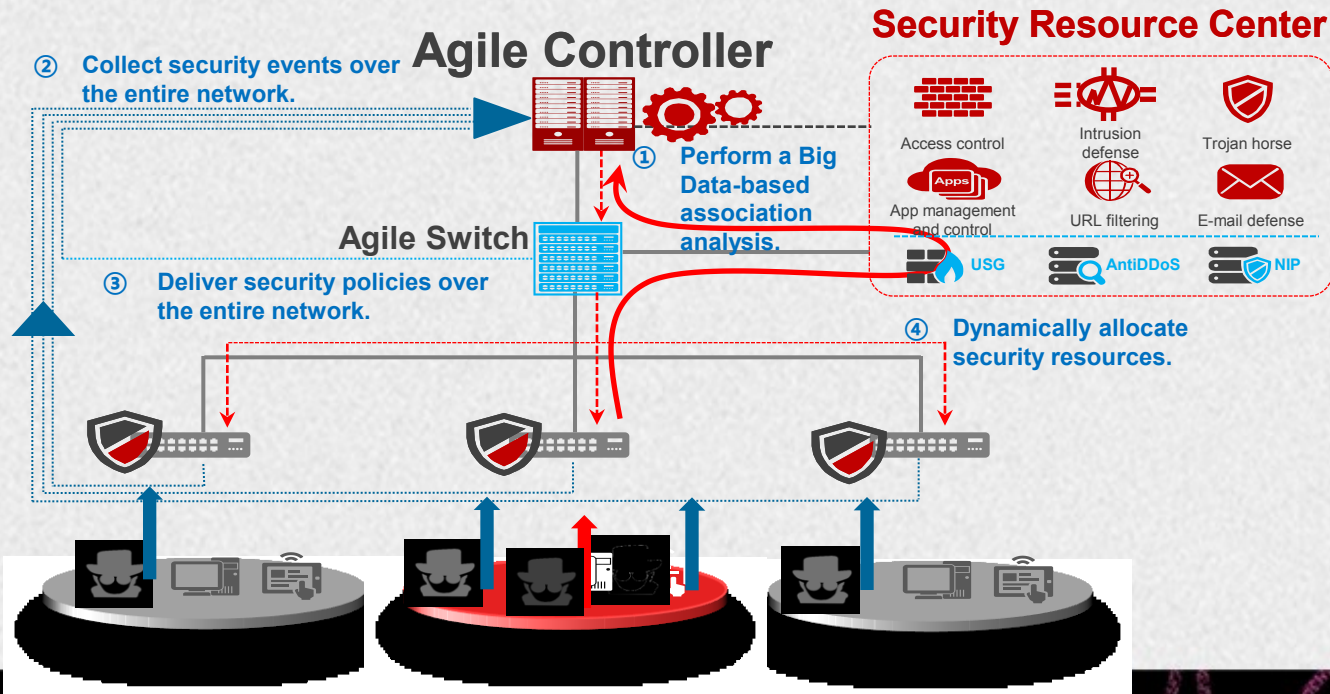
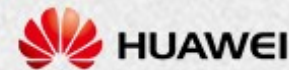
## Security Intelligence Center

- Maintains generation of security competence and smart security defense.
- Automatic threat sample analysis through tools.
- Accumulates global security reputation mechanisms by leveraging a Big Data platform.

# Big Data-based Security Defense System at the Enterprise Side



# Big Data Analytics-based Security Solution — United Security



**Awareness**

- ① Collect security events over the entire network
- ② Perform a Big Data-based association analysis

**Response**

- ③ Unified scheduling over the entire network
- ④ Delivery of security policies over the entire network

**Defense**

- ⑤ Dynamic expansion of security capabilities
- ⑥ Effective defense against unknown threats

..... Collect security events

..... Activate security policies

..... Traffic diversion

敏捷已来  
Weaving The Future



# Big Data Analytics-based Smart Management

## — Smart Policy@USG6000



### Learning

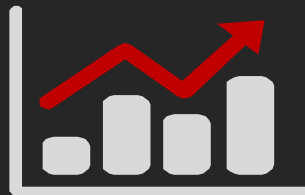


Learn and analyze large traffic volumes

#### Real-world traffic learning

- Learn service traffic on the entire network.
- Analyze the service traffic composition.

### Data Mining



Create network application models

#### Create conventional models based on traffic learning

- Discover and collect network use habits.
- Create conventional application models.
- Security competence overlapping and matching.

### Proposal



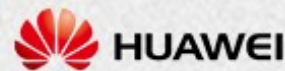
Big Data analytics-based policy proposals

#### Automatic policy generation and simplified management

- Automatically generate application-layer policies based on traffic and common traffic models.

# Big Data Analytics-based DDoS Attack Defense

## — AntiDDoS8000/1000

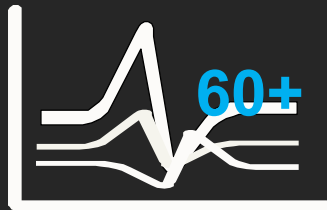


### Capturing



Packet-by-packet detection  
of all traffic

### Analysis



Analysis of 60+ traffic  
models

### Reputation



Complete reputation  
mechanism

**Full-scale analysis depends on full-scale traffic extraction.**

- 100% all traffic detection
- Packet-by-packet detection at Layers 3 through 7

**Accurate analysis results depend on full-scale analysis.**

- 5 dimensions
- 8 protocol suites
- 38 protocol statuses
- 60+ traffic models

**Big Data-based reputation mechanism allows highly efficient traffic processing.**

- Global Botnet IP reputation
- Proactive Botnet defense feature library

# Big Data Analytics-based Identification of 6,000+ HUAWEI Types of Applications — USG Full-Series NGFWs

## Learning

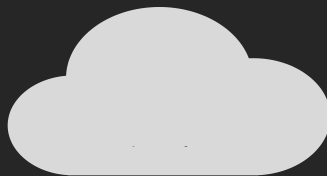


Global massive data learning

### Global application coverage

- Obtain global data through the global security competence center.
- Real-time data upgrade and quick coverage of new applications.

## Analysis



Cloud-based data analytics

### Real-time analysis and upgrade

- 24-hour cloud-based analysis.
- Obtain the latest application features.
- Discover potential security risks in applications and establish correlations.

## Feature



Global synchronization of application identification capabilities

### Information sharing and collaborative security protection

- Global application information can be updated and synchronized to the NGFW, DCFW, and UTM devices deployed by Huawei across the globe in real time.



# Huawei Security Product Family

## Security Service

### Competence Center

Botnet signature database	Spam library
Application protocol category database	URL category database
Virus/Malicious code signature database	Intrusion/vulnerability feature library

### Service Center

Security emergency response	Security management center
Online upgrade platform	Security management service
Reputation evaluation platform	Security consulting

## DC/Cloud Security

### Data Center Security Gateway



USG9500

Terabit DCFW

### DDoS Attack Defense



AntiDDoS1000/8000

Reputation Mechanism

### WAF



WAF2000/5000

## Campus Security

### NGFW



USG6300/6500

USG6600

6,000+ Applications

### IDS/IPS



NIP2000/5000

### UTM



USG2000/5000

### Security Access Gateway



SVN2000/5000

### Online Behavior Management



ASG2000

### Security Card



S Series Switches

## Terminal Security



**Policy Center**  
TSM



**AnyOffice**  
Mobile Terminal Client

## Security Management



**eSight**  
Unified Network Management

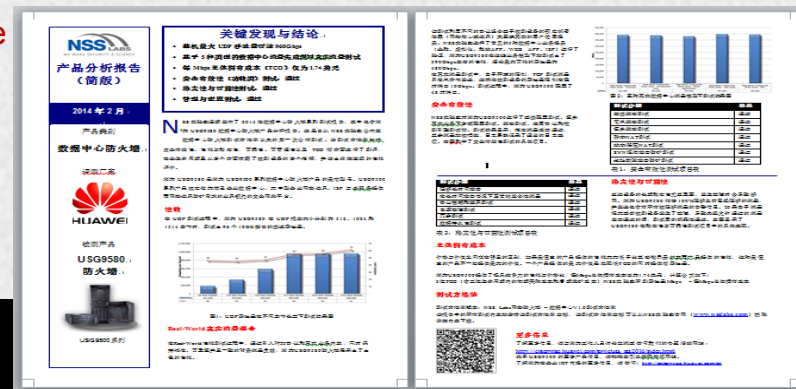


**UMA**  
Unified O&M and Audit

# Fastest Data Center Firewall (DCFW) — USG9500

"Huawei's USG9580 data center firewall is currently the test firewall that we have tested. We believe that security professionals, and anyone considering Huawei's solutions, will be very interested reviewing these results."

**Vikram Phatale**  
CEO of NSS Labs Inc.

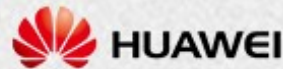


## Performance of the entire USG9580 device:

Maximum throughput: **960 Gbps**  
Maximum number of concurrent connections: **960 million**  
Maximum number of new connections per second: **12 million/second**  
3DES performance (3DES): **560 Gbps**  
HTTP performance (HTTP): **380 Gbps**



# Security Protection for the Egress of Peking University Campus Network

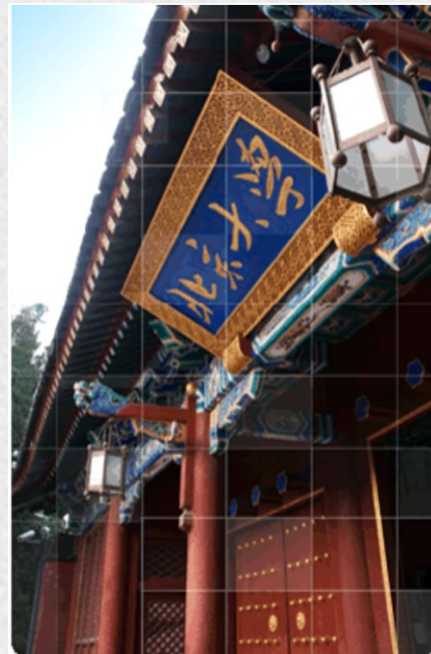


## Customer Requirements and Challenges

- Peking University has over **40,000** teachers and students. **47,000** computers are working over the University's campus network. The University's old network had poor stability and scalability and was overburdened during peak hours.
- The university has CERNET and CERNET2 networks and lacks **IPv4/IPv6** dual-stack-capable network security devices.

## Huawei Solution

- Huawei deployed its USG9500s on the egress of the University's campus network to meet the service access requirements during peak hours. The forwarding performance of the USG9500 can be linearly increased by adding boards.
- The USG9500s deployed on the egress support IPv4/IPv6 dual stack and therefore meet the requirements of education, R&D, and public network access.





# Powerful Anti-DDoS Solution — AntiDDoS8000



Frost & Sullivan "2012 Product Innovation Award"



## Industry's Most Accurate Anti-DDoS Solution



**Anti-Large-DDoS:** Each device provides a maximum of **1 Tbps** defense performance.



**Anti-App-DDoS:** Defends against **100+** types of DDoS attacks.



**Anti-Mobile-DDoS:** Defends against **mobile** DDoS attacks.



**Anti-Outbound-DDoS:** **Blocks attacks at the source.**

## Industry's Highest-Performance Anti-DDoS Solution

	Huawei	Industry
Types of DDoS attacks	100+	30+
Highest defense performance	1 Tbps	40 Gbps
High praises from customers	 Tencent	 Equinix  Alibaba

# Huawei Anti-DDoS Solution for Tencent's Data Centers



## Customer Requirements and Challenges

- Tencent's abundant services are transmitted in its data centers throughout China. Tencent has hundreds of millions of users. Even one-second service interruption will cause a huge economic loss to the company.
- On the Internet, many attacks including traffic attacks and application-layer attacks threaten Tencent's data center networks.
- DNS attacks repeatedly occur on Tencent's networks, with the largest volume of traffic reaching 10 Gbps, which severely affects Tencent's services.
- Tencent urgently need high-performance, high-precision, and professional anti-DDoS products to defend against DDoS attacks.

## Huawei Solution

- Huawei Anti-DDoS Solution provides professional hardware platform, excellent performance, fine-grained threat and attack defense, rapid response mechanism, and flexible deployment mode for Tencent and outperforms in Tencent's strict tests and live network application, winning a high praise from the customer.



# Most Innovative NGFW — USG6000

Horizontal evaluation by  
Network World: No. 1

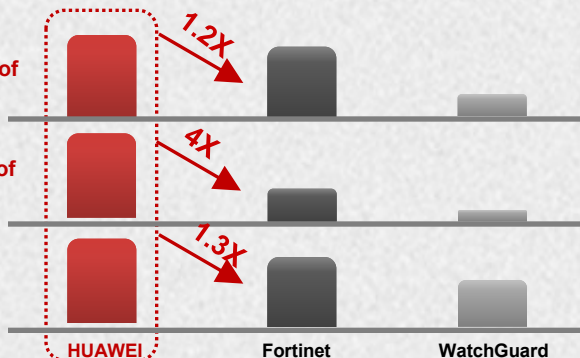
**NETWORKWORLD** No.1

**Performance:  
No. 1**

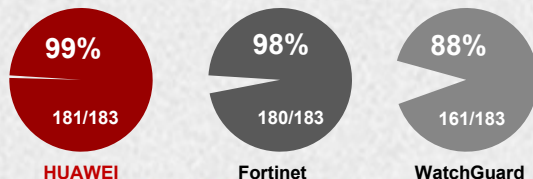
Maximum number of  
concurrent  
connections: No. 1

Maximum number of  
new connections  
per second: No. 1

Throughput: No. 1



**Threat detection  
rate: No. 1**



**NGFW USG6000**

**6,000+**

Application identification:  
industry's **No. 1**

Smart policies: **only Huawei  
USG6000** in China

Since its rollout in 2013, Huawei USG6000 has won multiple  
technology innovation awards:



"CIO's Trusted Excellent Product Award" in 2013



"Innovative Product of the Year" in 2013



"NGFW Innovative Product Award" in 2013



"Technical Excellence Award of the Year" in 2013



敏捷已来  
**Weaving The Future**



# Dortmund Stadium Campus Security

## Customer Requirements and Challenges

- Data center is threatened network attacks. As a result, smooth operations of key services such as online gambling and video backhaul cannot be ensured.
- Football fans use the stadium network to access illegal networks, resulting in legal risks.
- It is challenging to use limited leased bandwidth to provide satisfactory online experience for 800,000 football fans during games.

## Customer Benefits

- Huawei deploys its USG6650 series NGFWs at service system borders and USG6680 series NGFWs in the data center. These series NGFWs are enabled with functions of DDoS attack defense and application-layer attack defense.
- USG6000's traffic management function is used to limit traffic of Point-to-Point (P2P) applications to guarantee bandwidth for key service traffic forwarding. The USG6000 associates with the Terminal Security Management (TSM) system to identify users, providing differentiated network access experiences for VIP users and common football fans.





# THANKS

敏捷已来

**Weaving The Future**

*Envision A Better Connected World*



# Media Evaluations

## ■ Terabit DCFW USG9500

- Won ZOL's "Excellent Product of the Year" award for 2013
- Won PilotHouse's "Market Challenge Award" in 2012

## ■ NGFW USG6000

- Won China Network World's "NGFW Innovative Product Award" in 2013
- Won IT168's "Technical Excellence Award" in 2013
- Won ChinaByte's "CIO's Trusted Excellent Product Award" in 2013
- Won China Computerworld's "Innovative Product of the Year" in 2013

## ■ Professional Anti-DDoS Products AntiDDoS1000/8000

- Won Frost & Sullivan "2012 Product Innovation Award"
- Won "CSO's Trusted Information Security Solution Award" from China Computerworld in 2012

