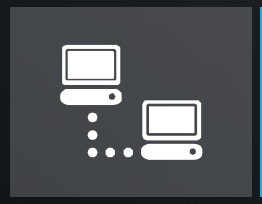
CANTO 2017

Cloud Sandboxing Against Advanced Persistent Attacks

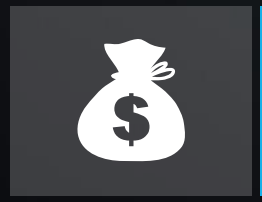
Ric Leung
Director of Product Management
Huawei Technologies Co., Ltd.

Traditional Defenses Are Ineffective Against Advanced Unknown Threats

Intensifying APT Attacks



Frequent Data Leaks



Considerable Financial Losses

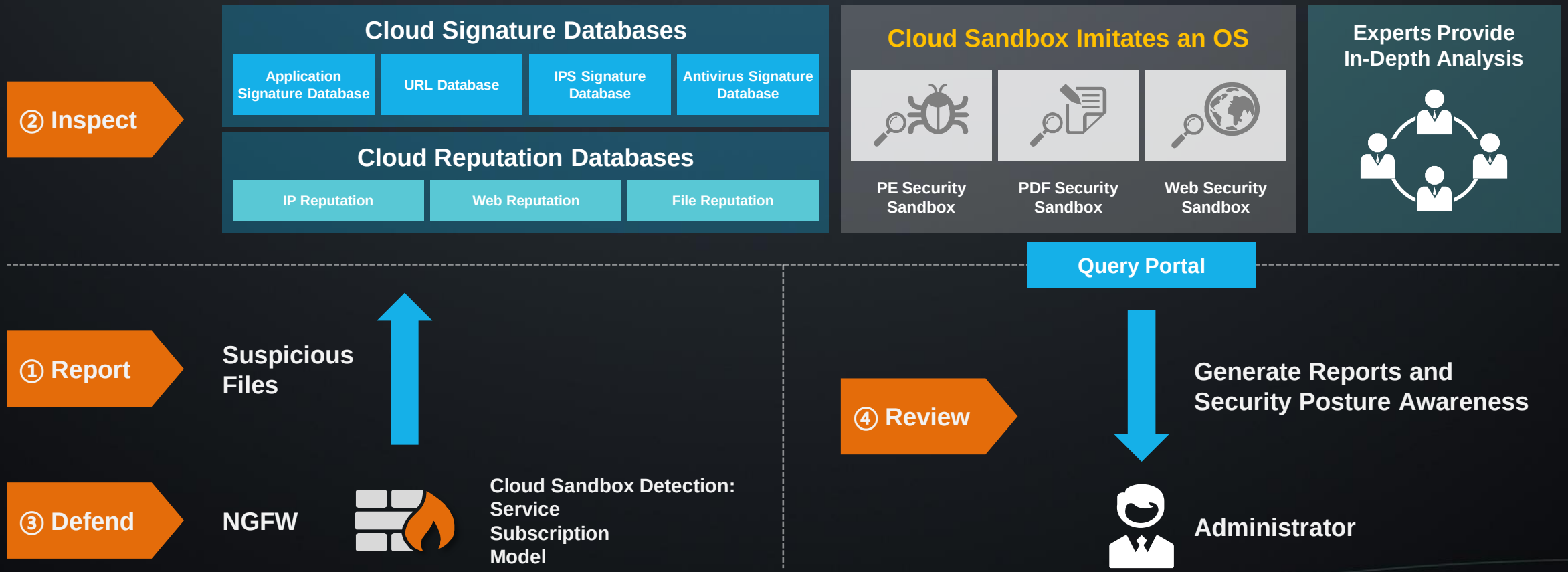
Ineffective Traditional Defenses

Sandboxed Defense of APTs

Cloud Sandboxing Enables Easy Defense Against Advanced Attacks

Rapid	Efficient	Comprehensive	Cost-effective
Deployment	Cloud Security	Detection	Independent from Hardware and Personnel Requirements

Integrated Cloud Sandboxing Defense System



Cloud Sandbox Security Capabilities Are Continually Updated

Cloud Sandbox

Emulate an actual environment to detect abnormalities

- Detects unknown malicious files, abnormal Command and Control (C&C)
- Horizontal scalability
- Cloud Sandbox Portal

Cloud Reputation

Identify reputation values of inspected items

- File reputation
- IP reputation
- Web reputation

Cloud Intelligence

Determine information about threats and attacks

- Domain queries
- File queries
- Reputation queries

Cloud Experts

Evaluate high-risk items for experts to analyze

- 24/7 professional support
- Important information provided for expert manual analysis

Cloud Security Posture

Assess network security situation

- Visual display of network-wide known and unknown threats
- Visual display of network-wide attacks
- Network-wide security posture awareness

Advantages of Cloud Sandbox

Rapid Deployment

Threat Visualization

Network-wide Detection

Ecosystem Partnerships

Rapid Deployment: One-click Advanced Threat Defense Subscription

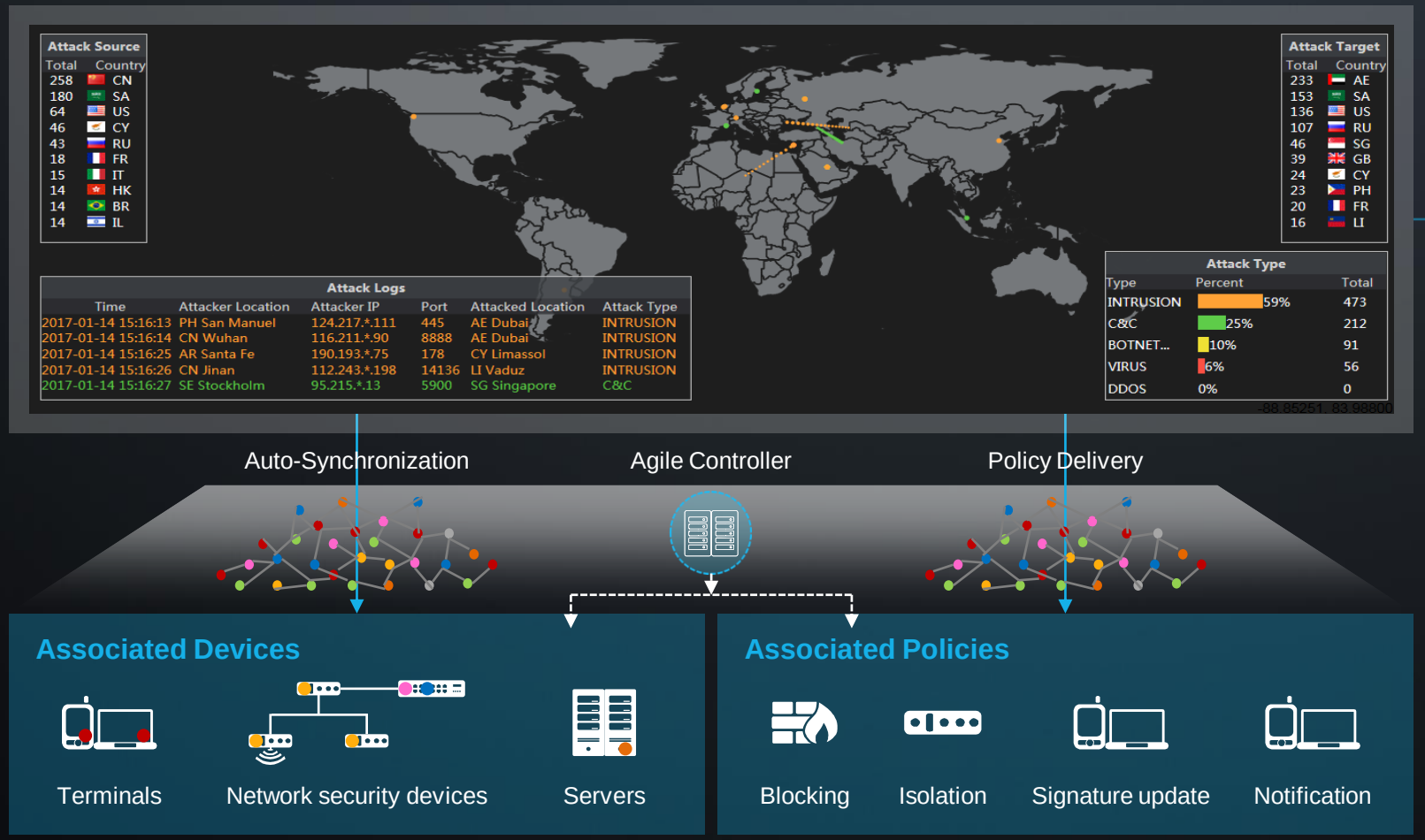
Sandbox Devices

- Specific device protection
- Online device deployment
- Expert administrators
- Configuration and maintenance
- Upgrades and expansion

Cloud Sandbox

- Uses existing network security devices
- Service subscription
- Zero configuration
- Expert analysis available anytime

Threat Visualization: Real-time Security Posture Display and Threat Prediction



Network-wide Threat Posture

- Overall security ratings
- City threat levels
- Rankings of assets by risk
- Rankings of countries by attack origin frequency
- Rankings of events by handling priority

Network-wide Detection: Leaves Unknown Threats with Nowhere to Hide

Identifiable Protocols	HTTP	SMTP	POP3	IMAP	FTP	HTTPS	
Identifiable File Types	EXE	Office	PDF	JS	WPS	RAR	40+ types
Simulated OSs	XP	Win 7	Win10				
Simulated Browsers	IE	Firefox	Chrome				
Simulated Office Versions	2003	2007	2010	2013	2016	WPS	
Simulated Adobe Reader Versions	R8	R9	RX	RXI			

- Cloud sandboxes can detect many file types and simulate many OSs.
- Ensures sandbox detection is accurate and comprehensive

Intelligence Sharing: Defends Against the Latest APT Attacks

CYREN

virustotal

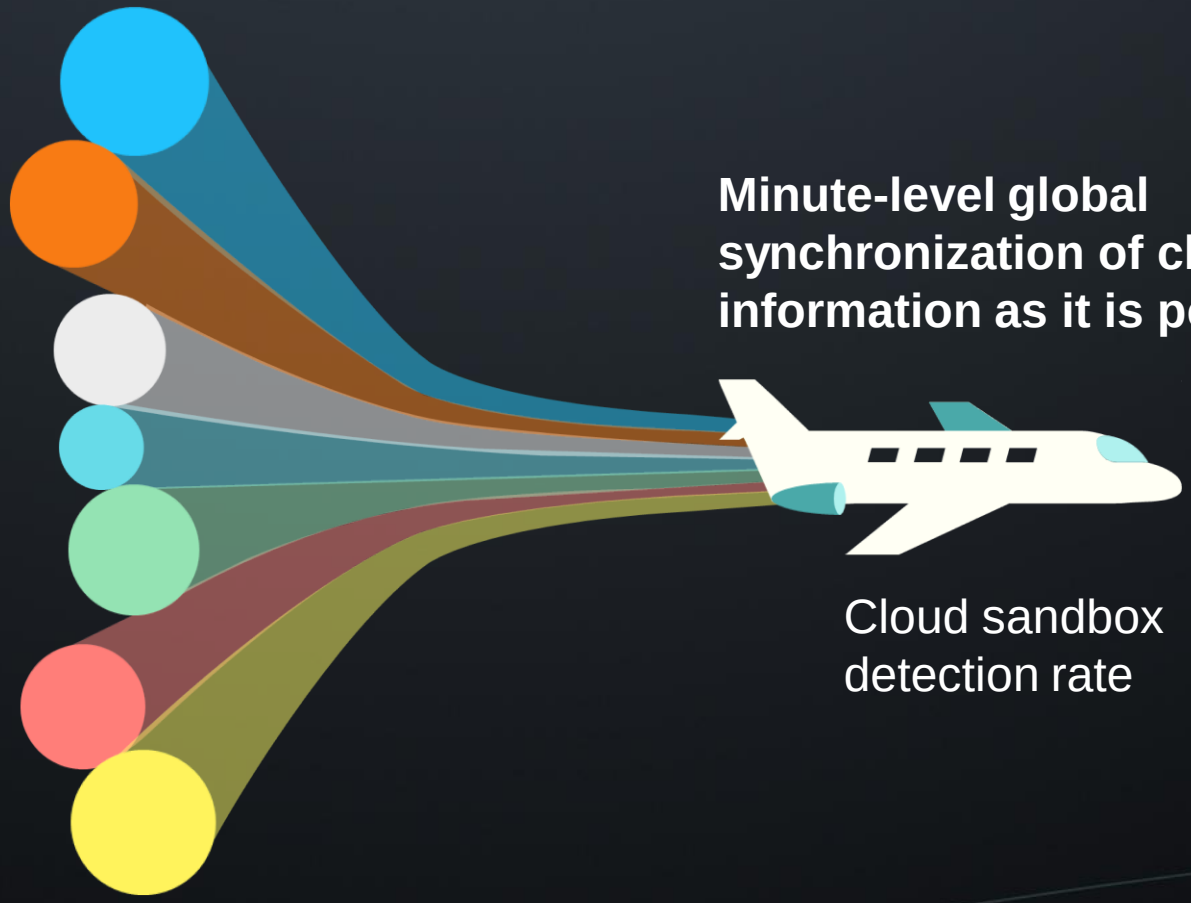
ThreatBook

Microsoft

IBM

CNNIC 中国互联网络信息中心 CHINA INTERNET NETWORK INFORMATION CENTER

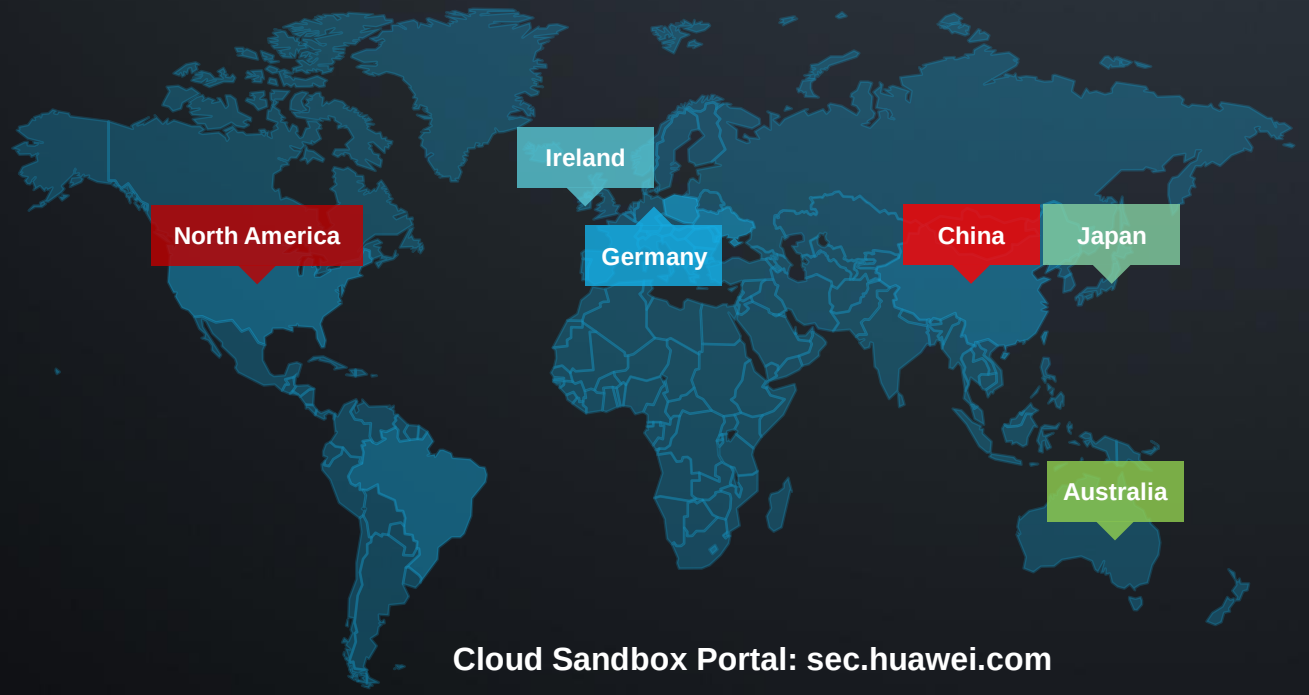
CN CERT/CC 国家互联网应急中心



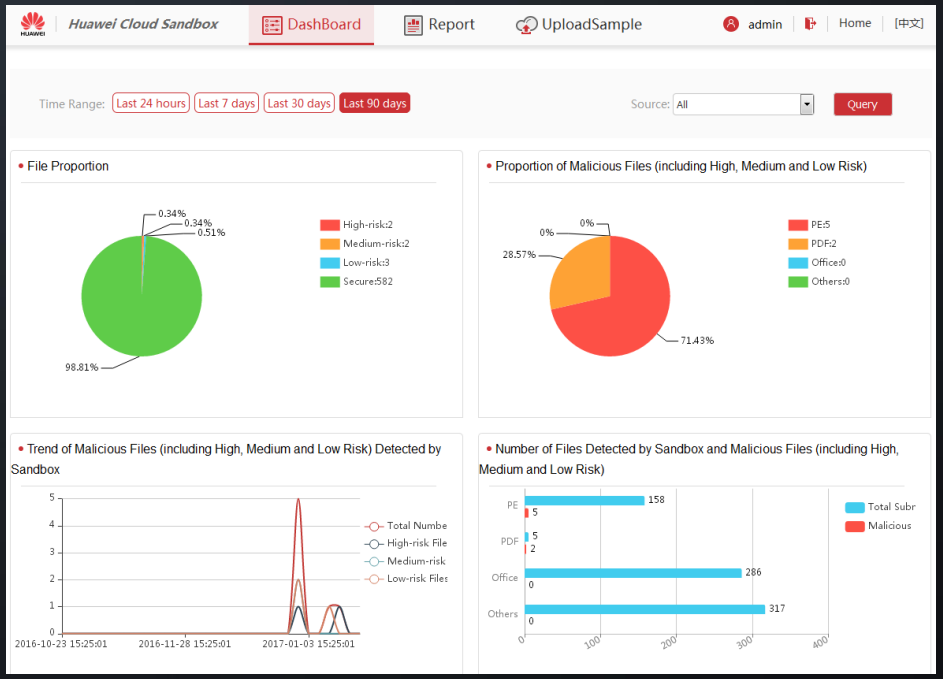
Minute-level global synchronization of cloud threat information as it is perceived

Cloud sandbox detection rate

Evolution of Huawei's Cloud Sandbox Deployment Around the Globe



Cloud Sandbox Portal: sec.huawei.com



Cloud Locations	Currently: China and Germany Planned: Ireland, Japan, North America, and Australia

Thank You.