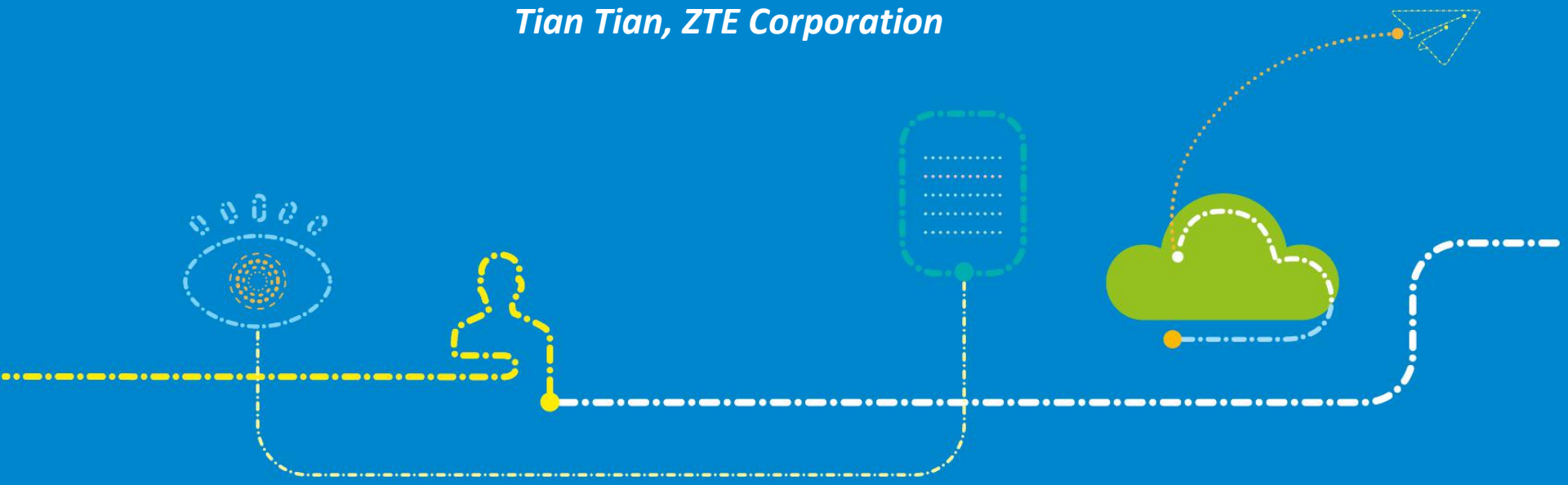
ZTE中兴

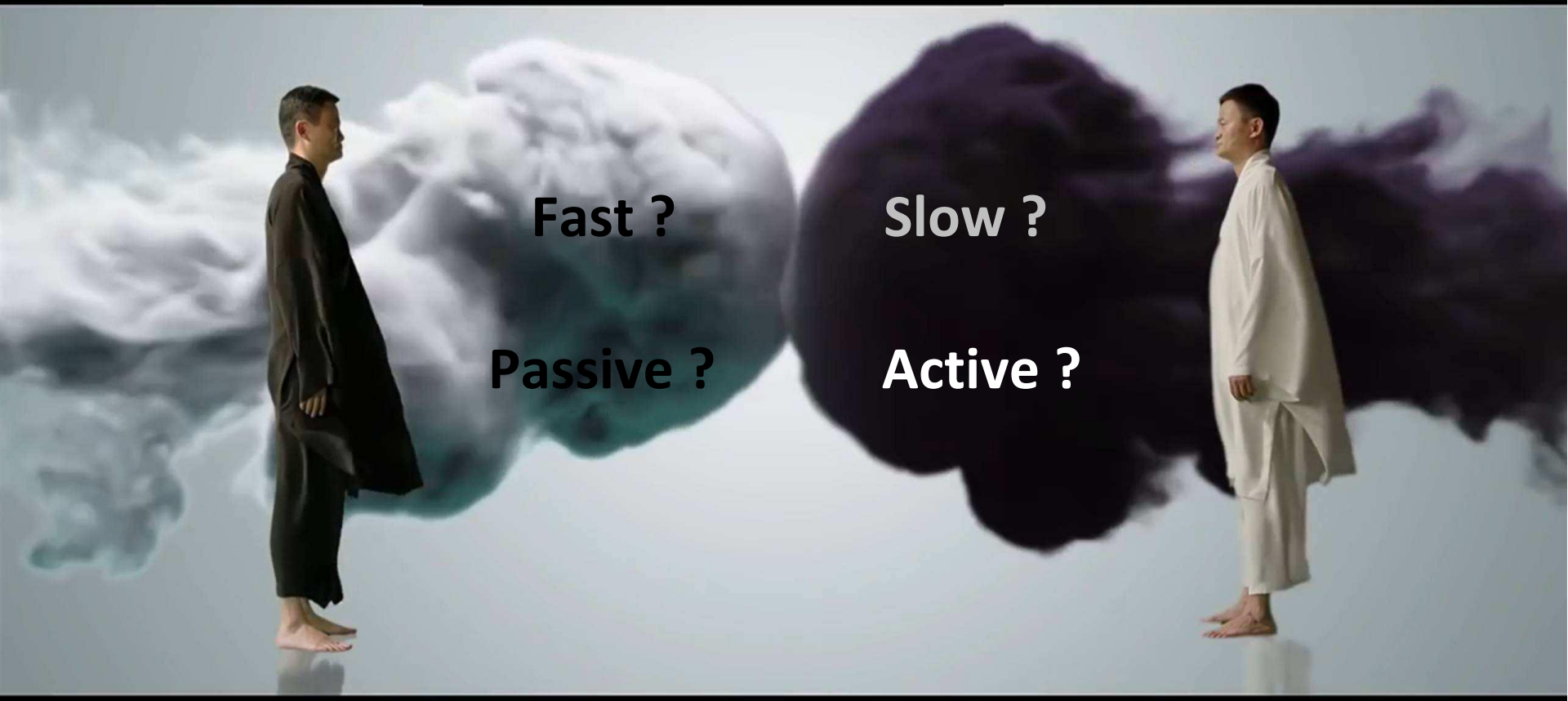
Unknown Threat Detection

--- the Key Ability of APT Defense

Tian Tian, ZTE Corporation



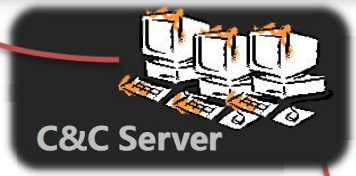
UNKNOWN



Detection ⟶ Response

APT Case Review --- RSA SecurID Breach

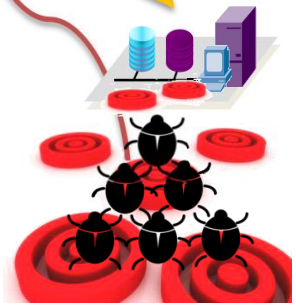
APT (Advanced Persistent Threat) attack against the world famous security company!



- Opened Email, opened malicous attachment ”2011 Recruitment Plan.xls”

- C&C Servers connections

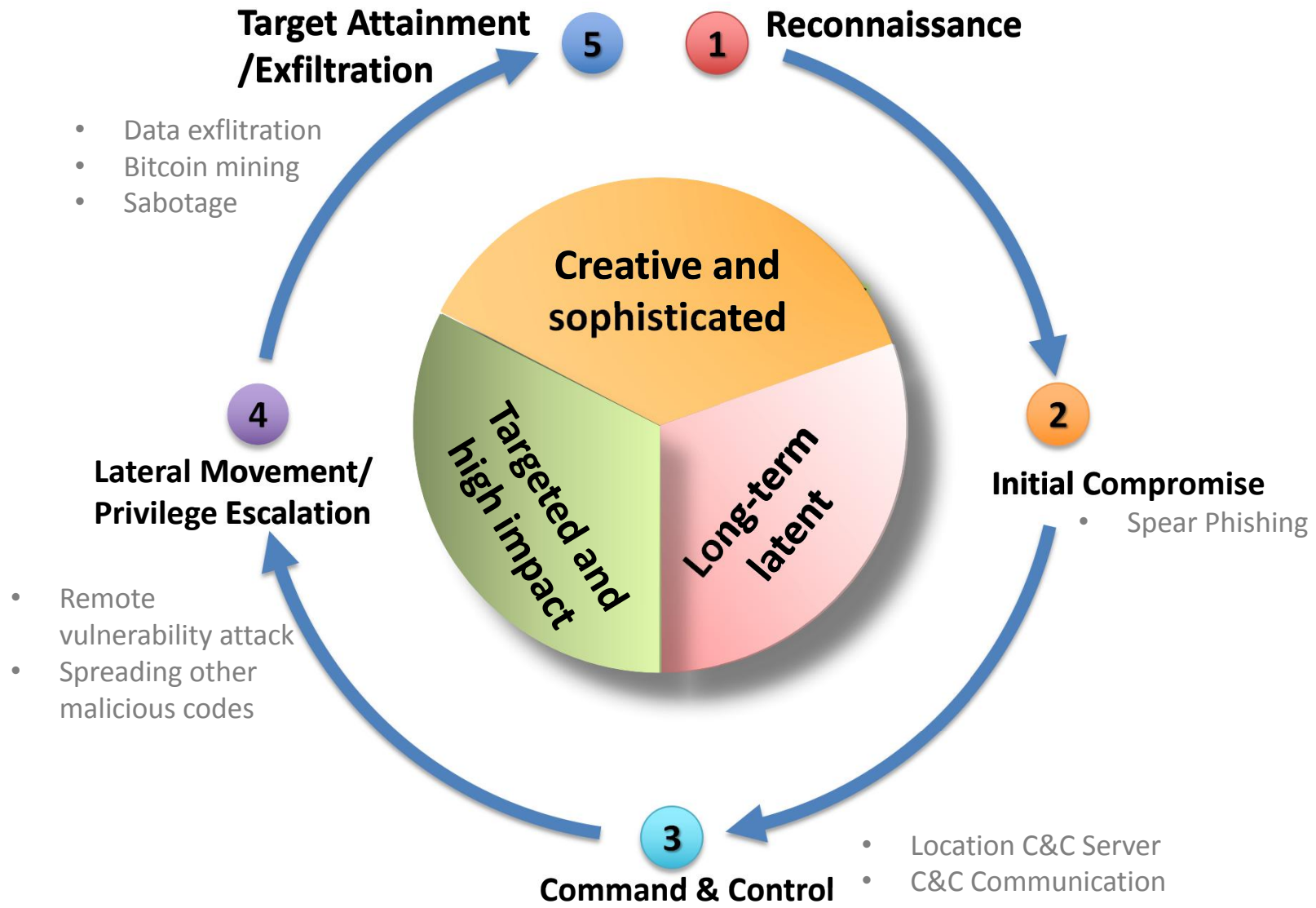
Spear phishing utilizing Adobe Flash 0Day vulnerability (CVE-2011-0609)



- Lateral movement
- Privilege escalation

- Exfiltrate SecureID data
- Remove attack traces

Advanced Cyber Attack Lifecycle & Features



Advanced cyber threats are hard to detect, new methods of detection and analysis are needed.

ZTE中兴

Advanced Attack Vs. Defense

Spear-Phishing

0-Day Exploits

Customed Malware

Malware Variants metamorphism &packer

Convert/Encrpted Tunnel

Socail Engineering

Unknown Threats

Firewall

IDS/IPS

Email-GW

Anti-Virus

Behavior Analysis

- Email attachments
- Web download files
- Other files

File Dynamical Behavior Analysis

Cyber Abnomal Behavior Analysis

- C&C Communication
- Internal abnormal access
- Abnormal data transmission

File Dynamical Behavior Analysis --- Sandbox Technology

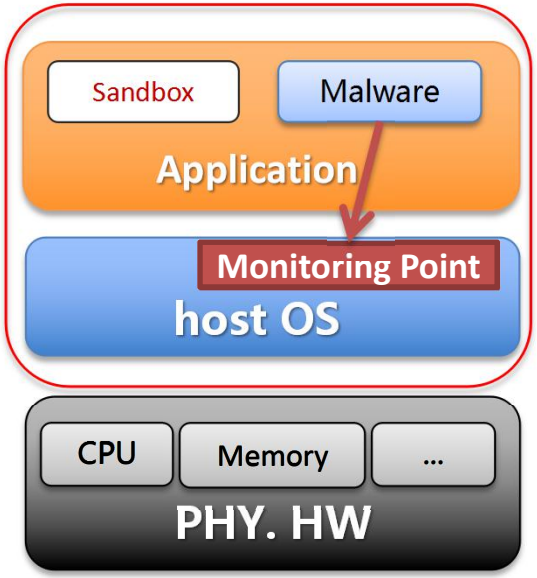
➢ Principle

- Use behavioral analysis methods to monitor unknown malware programs in a simulated/isolated environment

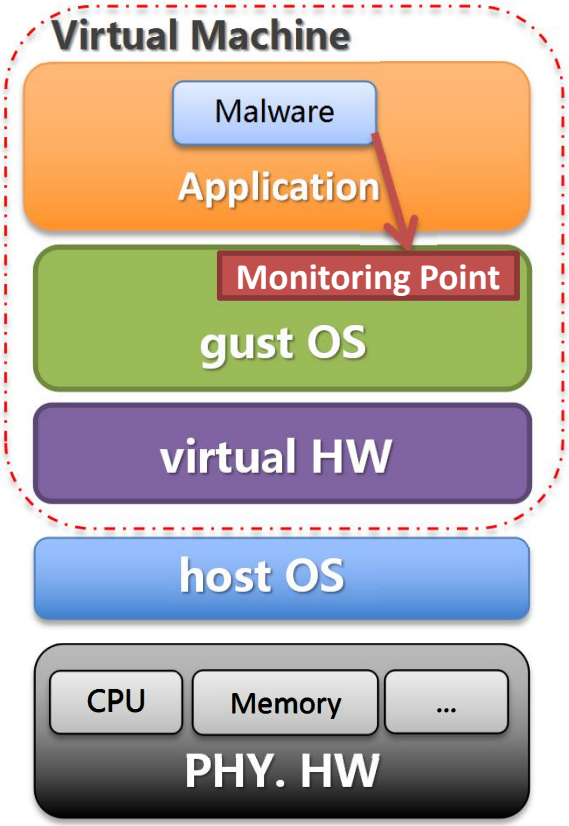
➢ Requirement

- High Level of Visibility into Malware Behavior
- Resistance to Evasion
- Scalability of Analysis and Management

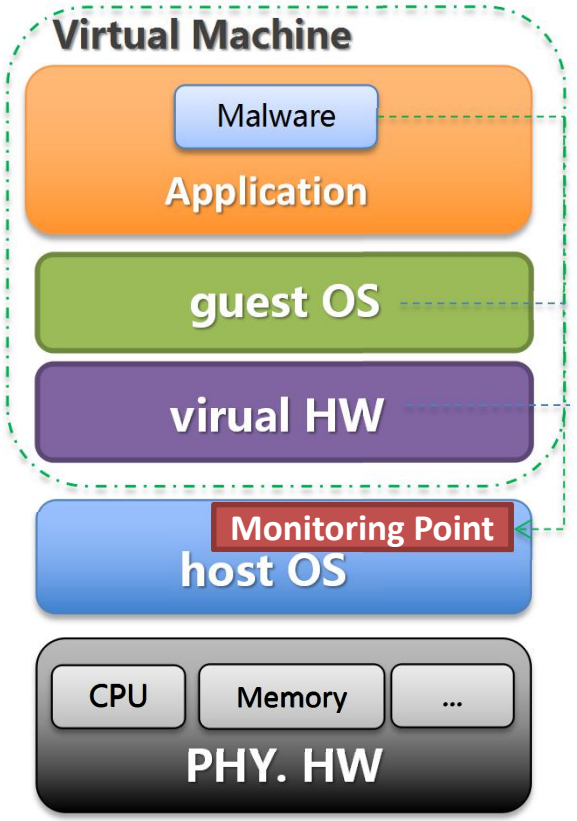
Sandbox Technologies



First-generation Sandboxing

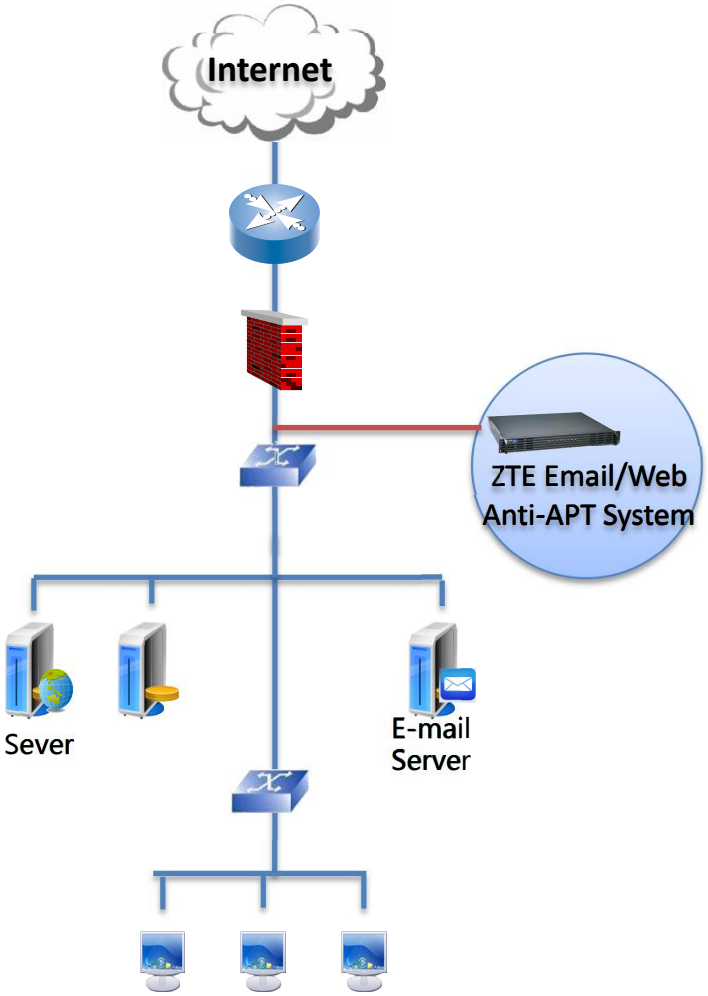


Second-generation Sandbox based on software virtualization



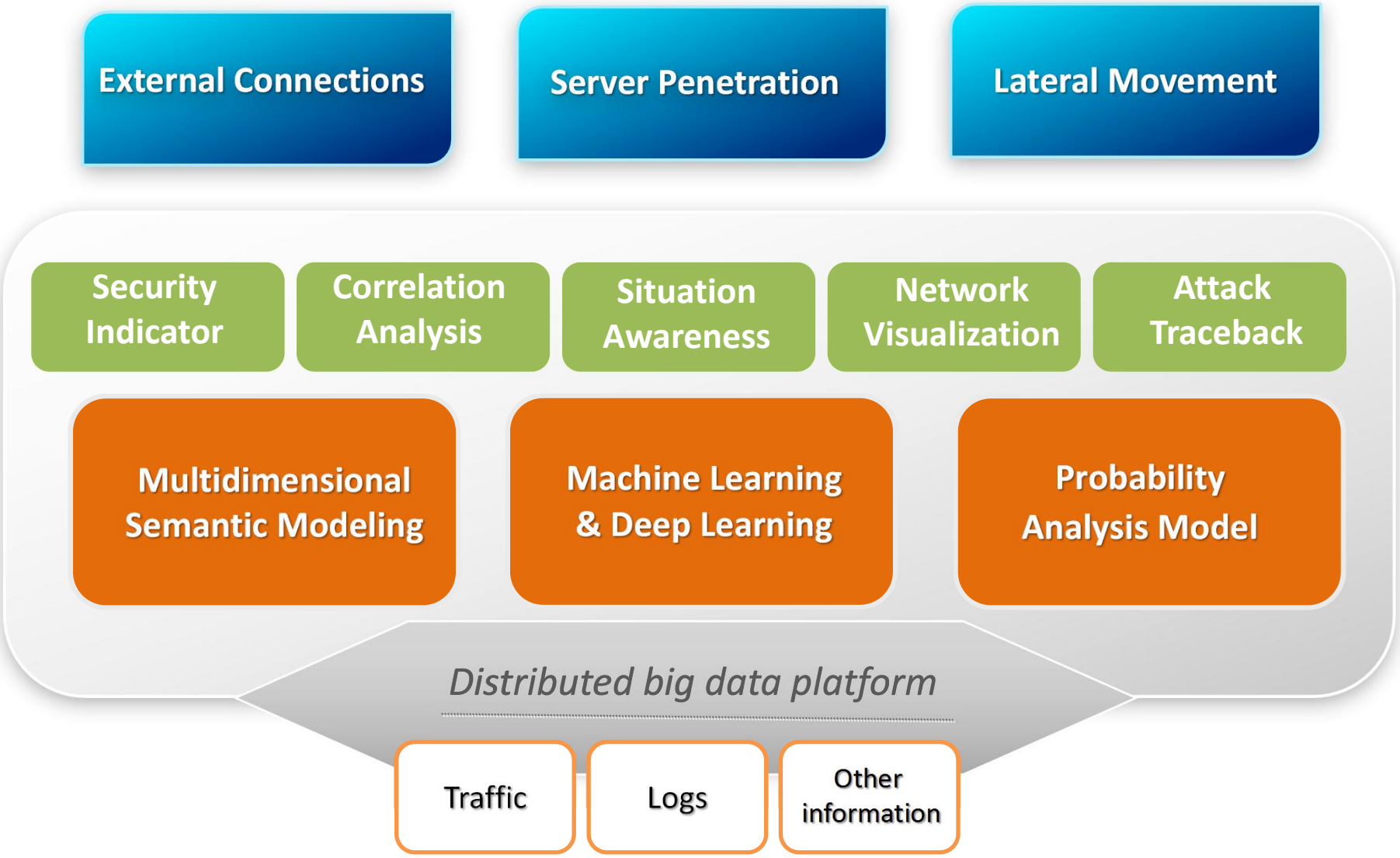
Third-generation Sandbox based on hardware virtualization

ZTE Email/Web Anti-APT System

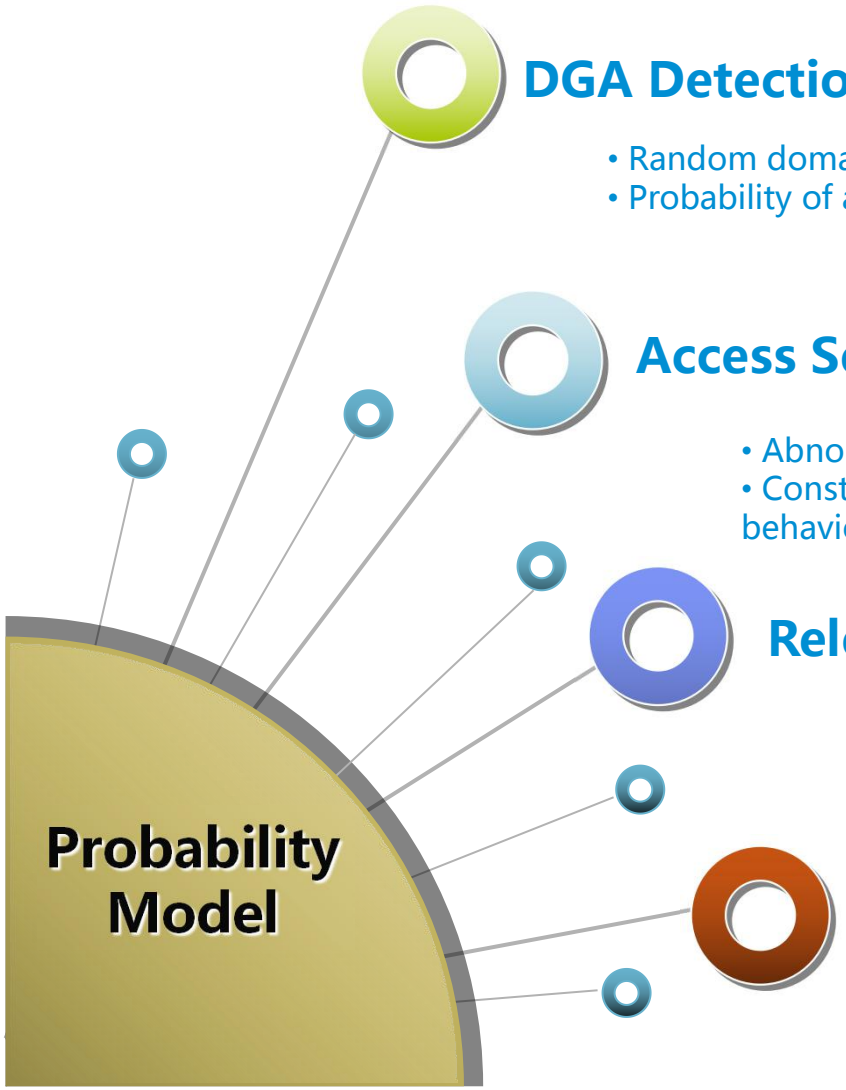


- **Easy deployment**
  - Common mode: parallel deployment
  - Analyze incoming traffic mirroring
- **Advanced technology**
  - Third-generation Sandbox technology based on hardware virtulization
- **Scalble Analysis and Management**
  - Support distributed deployment of dynamic analysis engines

Cyber Abnomal Behavior Analysis



Probability Analysis Model Design



DGA Detection Model

- Random domain names used to locate C&C servers
- Probability of a domain name belonging to DGA

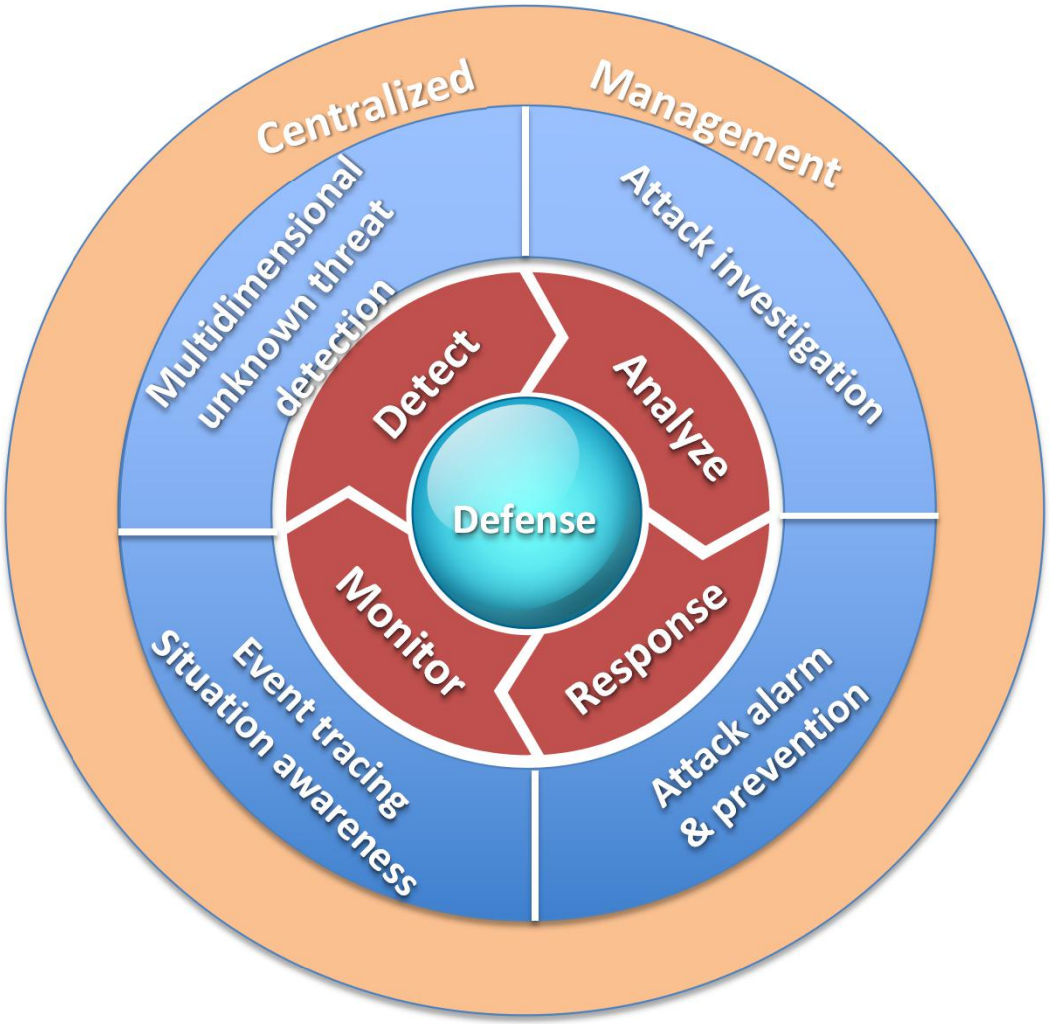
Access Sequence Detection Model

- Abnormal access behavior to the core resources
- Constructing transition probability matrix for behavior patterns

Relevance Detection Model

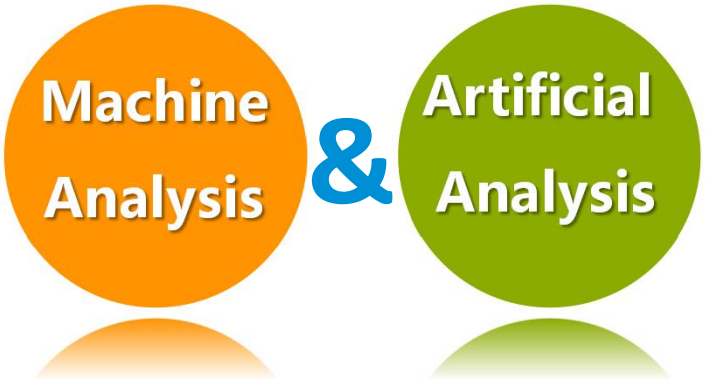
- Springboards and a series individual actions of malware attacks
- Temporal correlation of individuals, attack chain and scope suvey

ZTE Defense Solution Overview



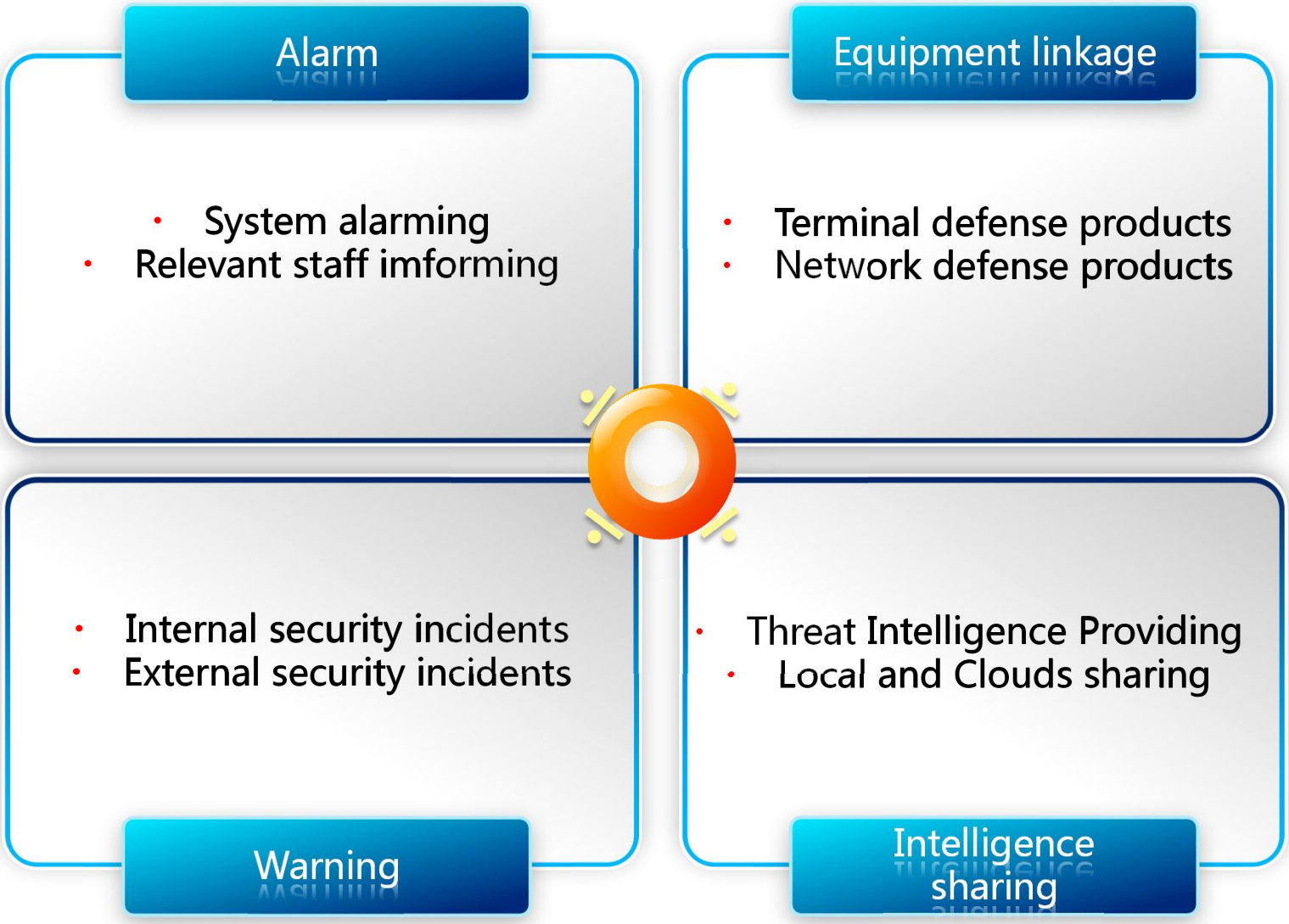
Analyze

- **Threat Extraction**
  - Statistics & Display
  - Sample deletion and management
- **Event Traceback**
  - Traffic storage
  - Log storage
- **Correlation Analysis**
  - Combination query
  - Visualization

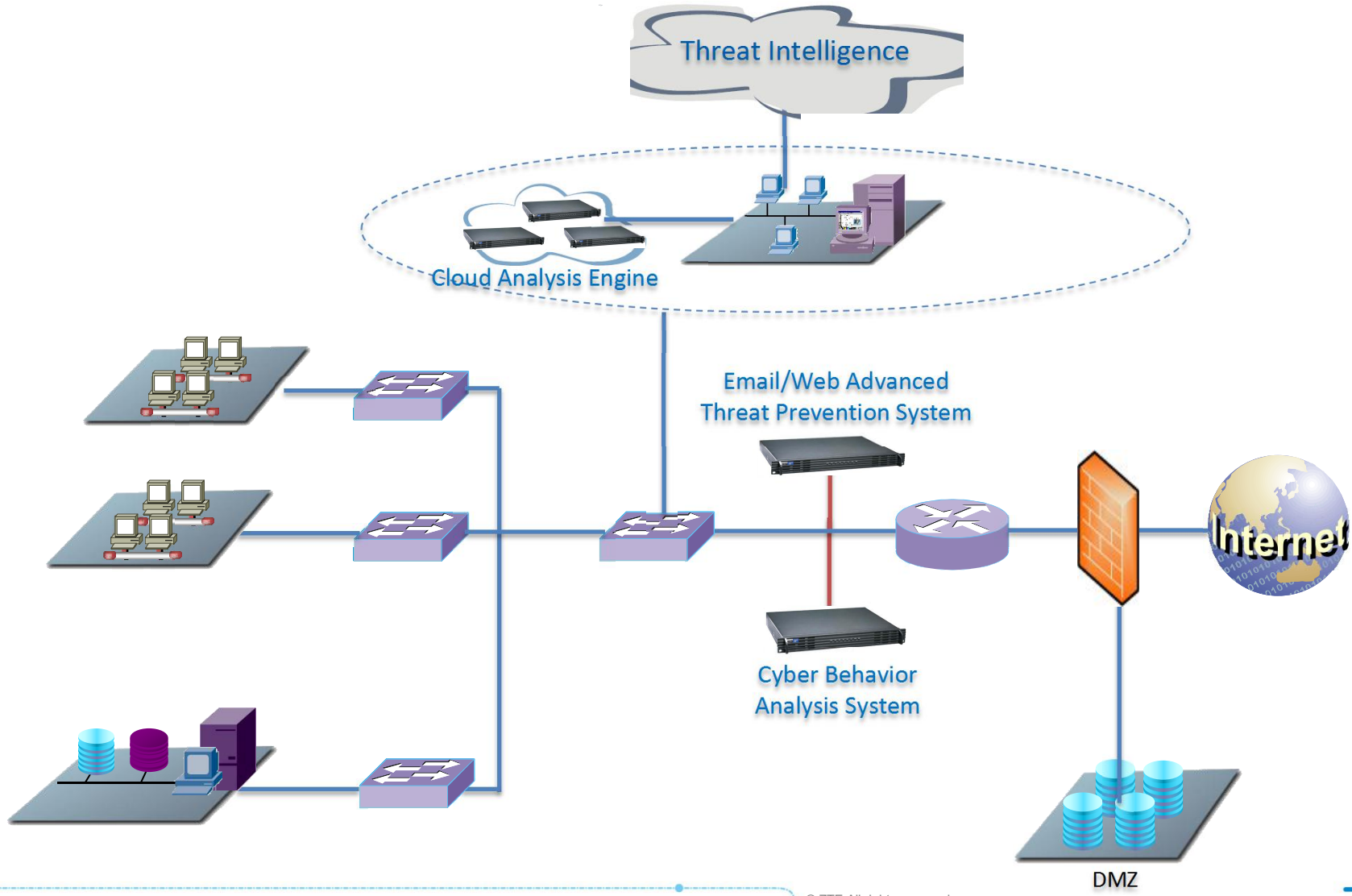


- **Important sample analysis**
- **Event investigation**
- **Threat Intelligence**
- **Defense rules deployment**

Automatic Response



Practical Deployment in ZTE



Practical Effect

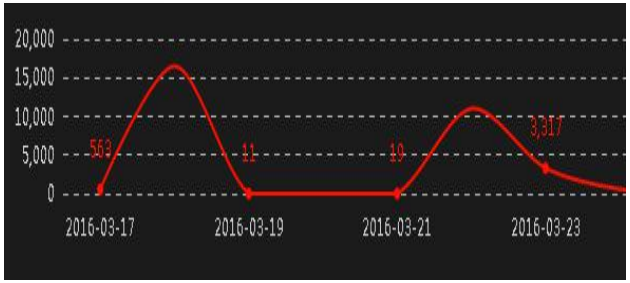
◆ **Successful detection and early warning of several advanced cyber attacks against ZTE**

Jan. 2017
Particular areas attack detected

Feb. 2016
Company executives targeted attack detected

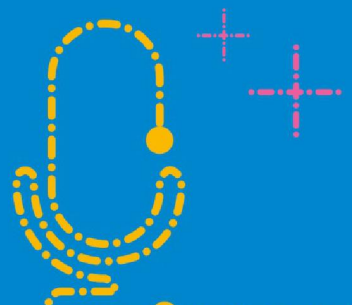
Feb.~Aug.2016
Continuous ransomware attack detected

Advanced Attacks cannot be detected by other traditional security products



- ***Highest daily detection number of ransomware: 10,000 +***
- ***Average daily high-risk malwares detected in email : 10 +(cannot be detected by most world famous antivirus software)***

Thanks !



5G 先锋