RSA Conference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SANGFOR

SESSION ID: GPS1-R08

New World, New IT, New Security

Jackie Chen

Chief Product & Marketing Officer
Sangfor Technologies (HQ)

#RSAC

New World, New IT, New Security

Internet of Things

Estimated **200 billion objects** in 2020 !

Source 1: IDC, Intel, United Nations.
Source 2: IDC & Gartner
Source 3: RightScale's Market Survey

BYOD

- Mobile Worker Population **1.3 million** in 2015.
- Tablets forecasted to reach **468 million** in 2017.
- Smartphones forecasted to reach **2.1 billion** in 2017.

Cloud

93% of organizations are running applications or experimenting with infrastructure-as-a-service.

The reality of cyber attacks

- Hacking of Hong Kong's VTech may prove worst cybersecurity breach of 2015 in Asia!

- LinkedIn Lost 167 Million Account Credentials in Data Breach !

- 55 million voters' details leaked in Philippines !

- Bangladesh bank governor resigns after $81m hack!

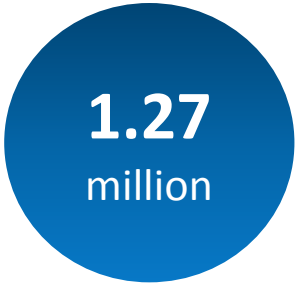
Cyber attack could kill people directly!

Cyber security challenges

Average number of reported alerts per week is 16,937, only about 4% of them are Investigated[1].

Average 200 Days to detect Security breach and 80 Days to Contain it[2].

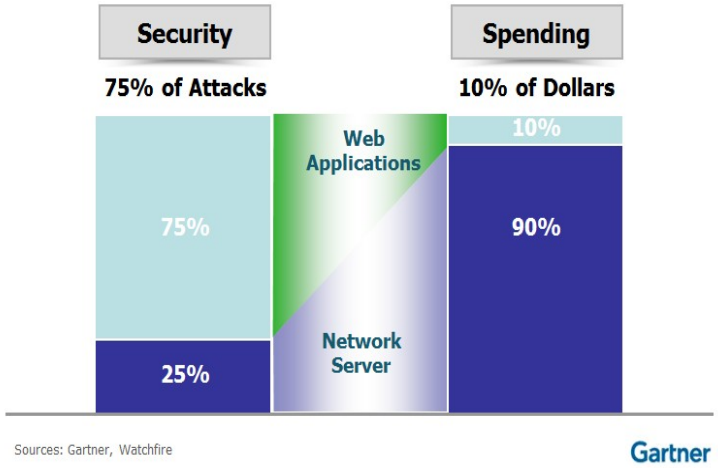
Average of 1.27 million US$ annually wasted[1].



Source 1: http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf
Source 2: https://blogs.windows.com/windowsexperience/2016/03/01/announcing-windows-defender-advanced-threat-protection/

Attack methods are shifting

Gartner estimates that 75% of attacks now take place at the application layer !



Source 1: Watchfire
Source 2: OWASP
Source 3: Gartner, NGFW & UTM 2015 Report

- "90% of sites are vulnerable to application attacks".
- "Application security is no longer a choice".
- "Gartner continually hears from clients that are seeing a 90% firewall CPU utilization after they enabled Web or email antivirus on the same platform. This impacts the user experience, with noticeably increased latency and reduced throughput."

SANGFOR

Traditional Security Model doesn't work any more

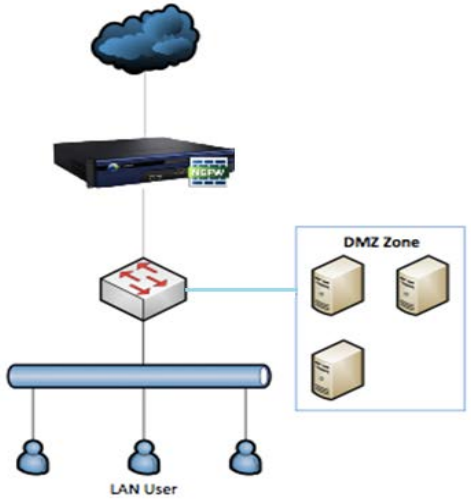
Experience sharing: Thailand Knowledge Park

Thailand Knowledge Park focuses on developing the learning opportunities and managing intellectual capital of Thailand. They create content in the form of digital books, videos and audios.

Challenges:

- Existing UTM Firewall doesn't offer enough performance when enable app security
- No Protection for their online websites but too expensive to have dedicated WAF device for website protection

Gateway + WAF



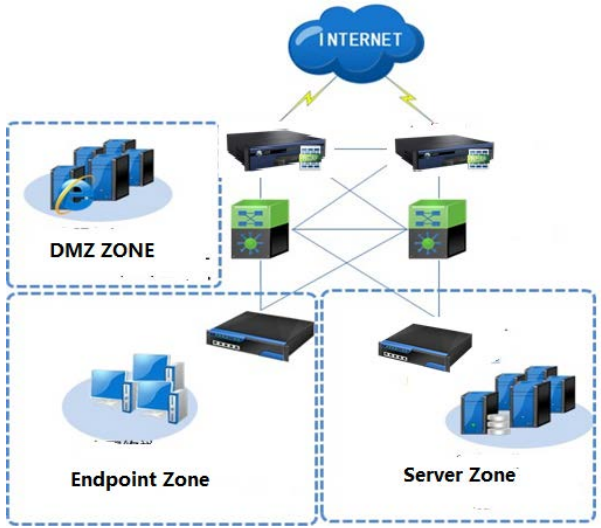
Experience Sharing: K.WAH Group, Hong Kong

Founded in 1955, K. Wah Group is an international company with market presence spanning Mainland China, Hong Kong, Macau, Southeast Asia and major cities in the US.

Challenges:

- Existing firewall provides poor security reporting tool for operation
- Concerns on new and emerging threats
- Business system vulnerabilities are not visible but risks are getting higher

Gateway with Vul. Visibility



SANGFOR

Experience sharing: Shen Zhen University

Challenges:

Don’t know real security situation

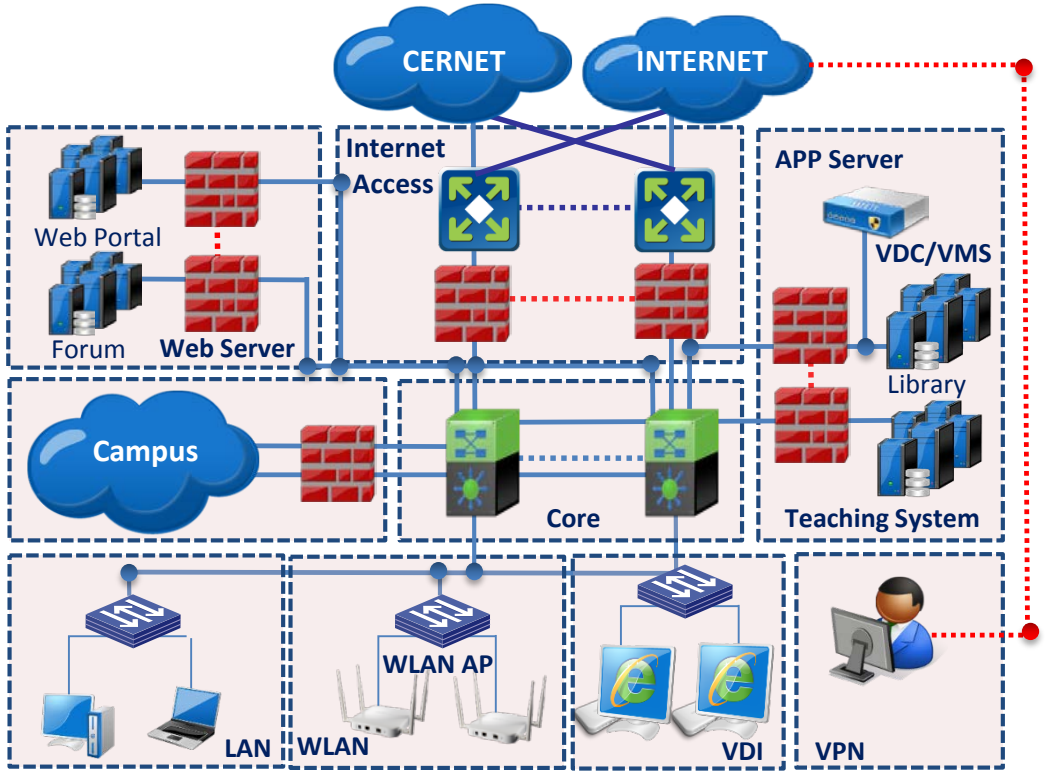
- 30,000 students and teachers.
- 45,000 endpoints
- 400 servers, Web servers, App servers.

8K+ logs and alerts weekly, almost no investigation

- Only few IT staff, most of them are junior professionals

Lots of attacks from internal network

- registration portal got tampered several times



SANGFOR

Key aspects of new security

Security Visibility

- Key Elements Visibility
- Intelligent Analyzing
- Management Visibility

Rapid Response

Real-time Detection

- Pre&Post-event detection
- Business risks detection

Rapid Response

- Automatic policy enforcement
- Solution synergy and Correlation
- Security expertise as a service

Simplified Security

Easy Deployment

- configuration wizard
- straightforward policy layout

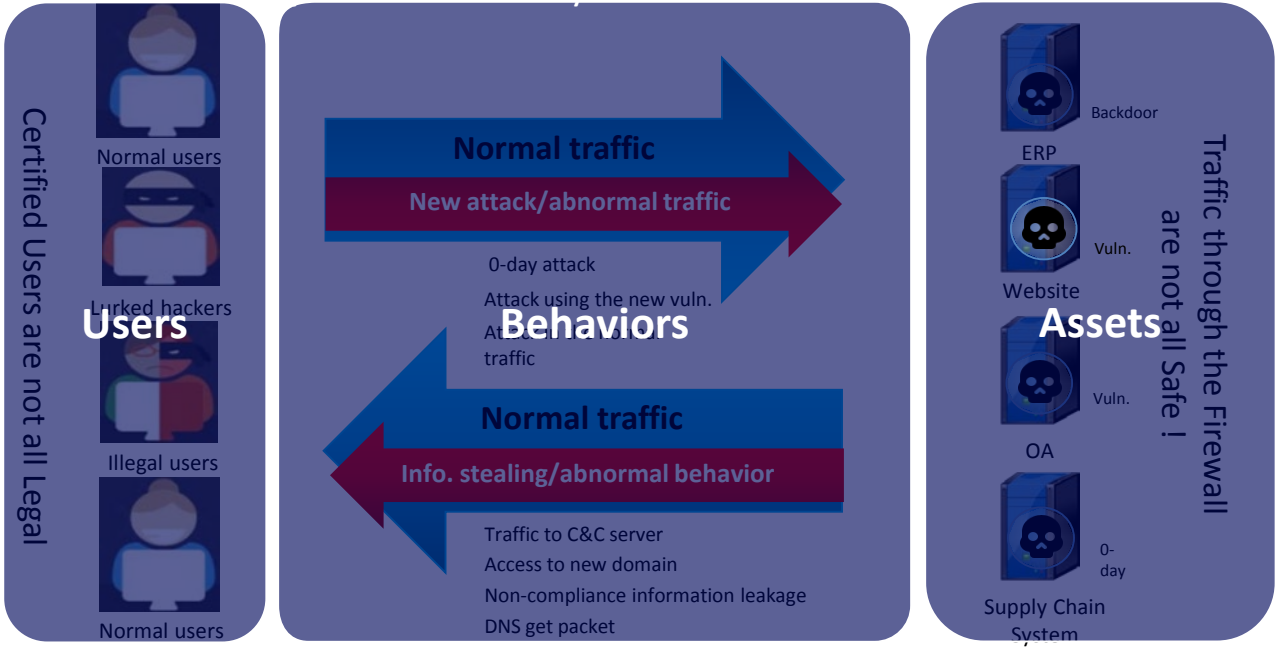
Simple O&M

- Intuitive security reporting
- Presented as security event
- Convergence

L7 High-Performance

- Hardware and software architecture
- Efficient algorithm

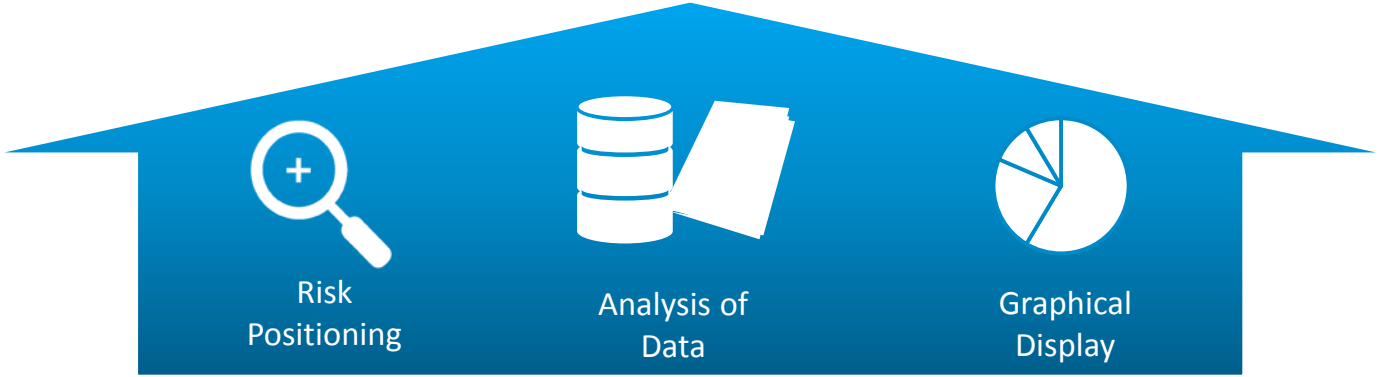
Visibility is the Foundation



Broader visibility, better security

accurate detect and defense

efficient security O&M



User Visibility

- User ID
- End-points
- Access mode
- Location

Behavior Visibility

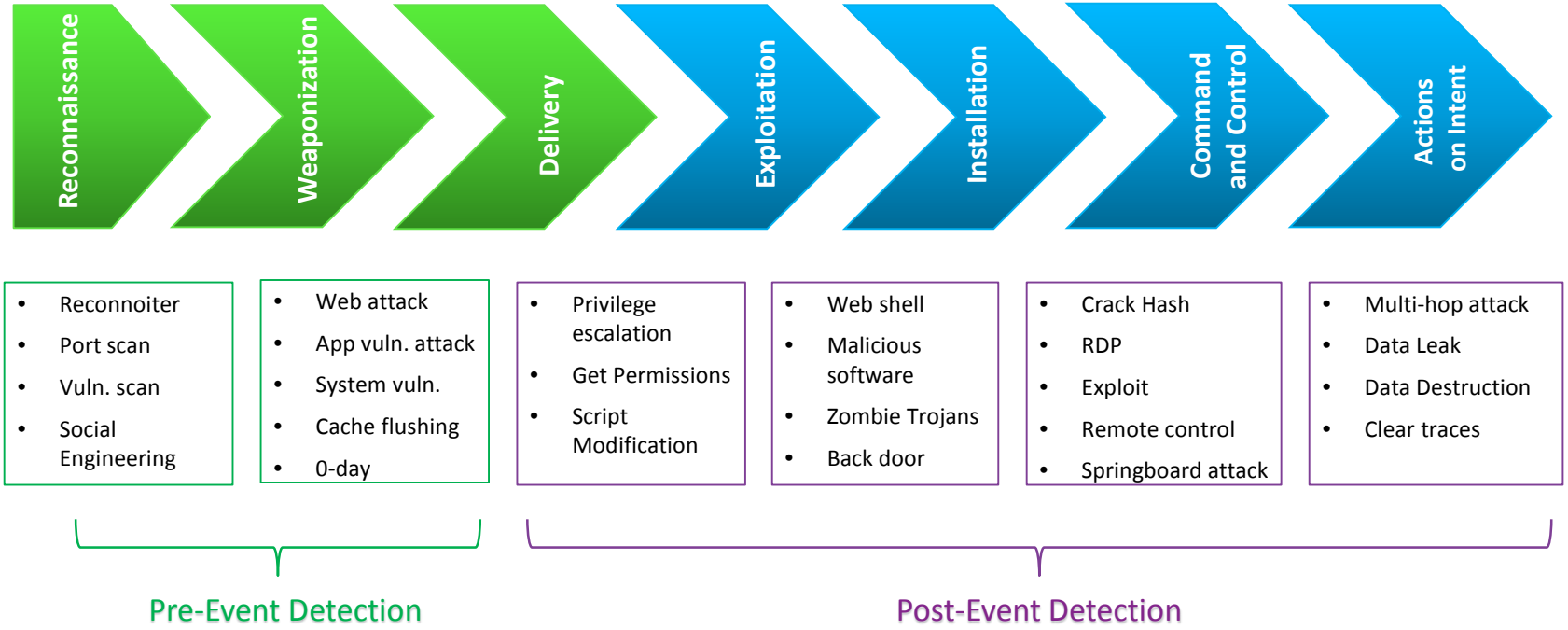
- Packet
- Traffic Log
- App
- Content

Business Visibility

- Location
- System Info
- Vuln.
- Data

SANGFOR

Real-Time Detection, fight to the death



Conclusion

New world and New IT demand New Security

- **Real Time Security Visibility** as the foundation
- **Fast response** to cut loss
- Simplify security operation **through convergence and intelligent automation**
- **Application layer Security** is the new security

Apply What You Have Learned Today

- **Following this presentation you should:**
  - Understand what are the key aspects of new security
- **Next week you should:**
  - Better understand your current security design and gaps with new security model
- **Within 3 months, you should:**
  - Start to fill in the gaps for better defense of cyber criminal

Thank you !

Jackie Chen

Chief Product & Marketing Officer

jackie.chen@sangfor.com

Your Security Guard to the Future