YOUR SECURITY GUARD TO THE FUTURE

NGAF FIREWALL PLATFORM

SANGFOR

Sangfor Technologies Co., Ltd.
www.sangfor.com

Table of Content

- **Security Trend**

– New Business, New Challenges

– Difficulties of O&M for Network Security

– New Security Model

- SANGFOR Security Concept
- NGAF – Your Security Guard to the Future

Cyber Risks: The Growing Threat

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

- LinkedIn Lost 167 Million Account Credentials in Data Breach !

- Megabreach: 55 million voters' details leaked in Philippines !

- About 40 attacks reported in last two months (2016), but one security firm says it detected 24,000 cases of Locky ransomware hacking attempts in March alone !

Source 1: http://www.scmp.com/tech/enterprises/article/1934188/asleep-wheel-cybersecurity-experts-continue-tirade-against-hong
Source 2: http://www.scmp.com/news/hong-kong/economy/article/1889604/hacking-hong-kongs-vtech-may-prove-worst-cybersecurity-breach
Source 3: http://fortune.com/2016/05/18/linkedin-data-breach-email-password/
Source 4: http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/

New World, New IT

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

Is security visibility Important ?

USERS

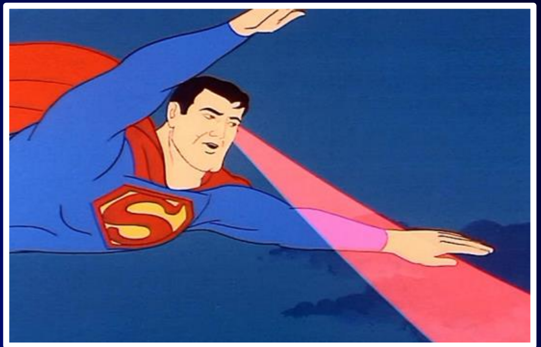
ATTACKS

VULNERABILITIES

BEHAVIORS

IT ASSETS

Not even Superman is able to see through Networks to find threats !



- “By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources.”

Source: Predicts 2016: Threat and Vulnerability Management, Gartner.

- If you really want to protect your network, you really have to know your network. You have to know the devices, the security technologies, and the things inside it.

Source: RSA Conference, Rob Joyce, NSA TAO Chief, Usenix Enigma 2016

What will happen without Real-Time Detection and Timely Response ?

Average number of reported alerts received per week is 16,937 and only about 4% of them could be Investigated.

16,937
alerts

Average 200 Days to detected Security breach and 80 Days to Contain it.

200
days

Average of 1.27 million US$ annually in time wasted

1.27
million

Source 1: Ponemon Institute study
Source 2: Ponemon Institute study
Source 3: Windows

Difficulties of O&M for Network Security

In average, an enterprise receives 16,937 alerts per week* !

*Source: Ponemon Institute Study of 630 enterprises

Without intelligent & automatic reporting tools, IT team has to read each report

IT team has to identify real & effective threats amongst thousands of alerts

After identifying the threat, due to lack of knowledge, IT team will waste time to find the right solution

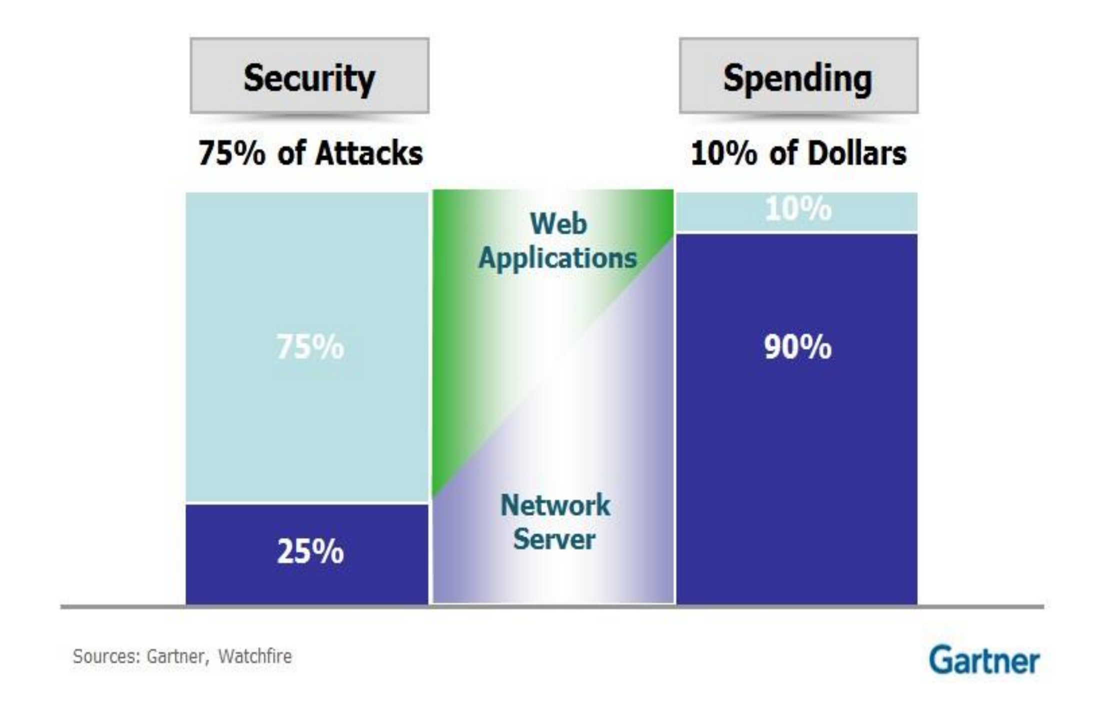
Cost Calculation (Cost per Employee)

Time wasted per day: 4 hours
Average pay per day: US$ 60
Average wasted money per day: US$ 30
Average wasted money per month: US$ 600
Average wasted money per year: US$ 7200

Not including the risk of employees missing important threats and related cost + reputation damage !

L7 Application Layer Issue

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



"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."

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

Traditional Security Model is Outdated !

No Visibility of Users, Traffic and IT Assets !

No Real-Time Detection, No Post-Event Detection, Slow Response !

Difficulties of O&M for Network Security, Time Wasted !

Low Performance for L7 Application Layer Security !

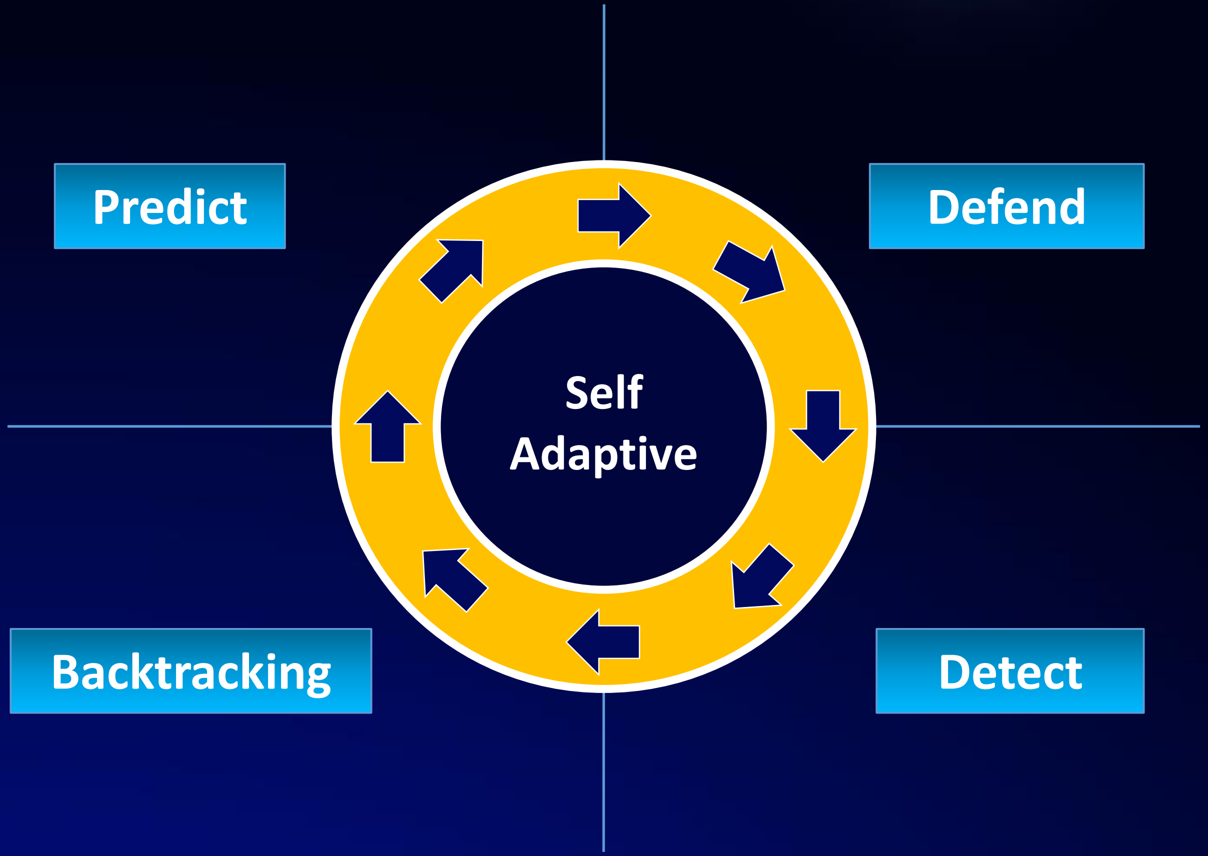
OUTDATED

Self-Adaptive Security Architecture

- Security is **more than just Defend.**

- Real-Time Detection at all phases to provide Real-time **Visibility**.

- **Fast Response and Automation** is the key to reduce Risks.



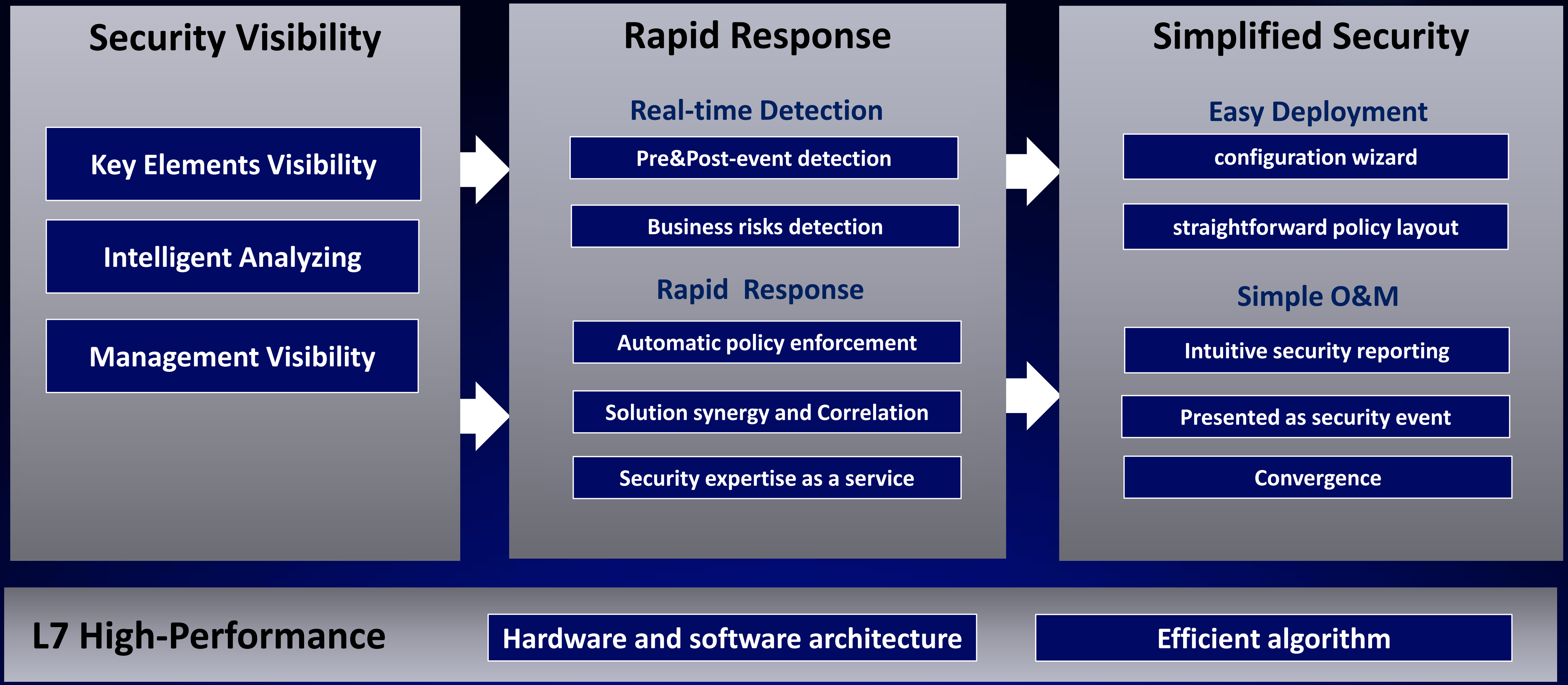
Source: Gartner

Table of Content

- Security Trend
- **SANGFOR Security Concept**
  – Security Visibility
  – Real-Time Detection, Rapid Response
  – Simple Security for O&M
  – L7 Security High Performance
- NGAF – Your Security Guard to the Future

SANGFOR Security Concept

SANGFOR



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

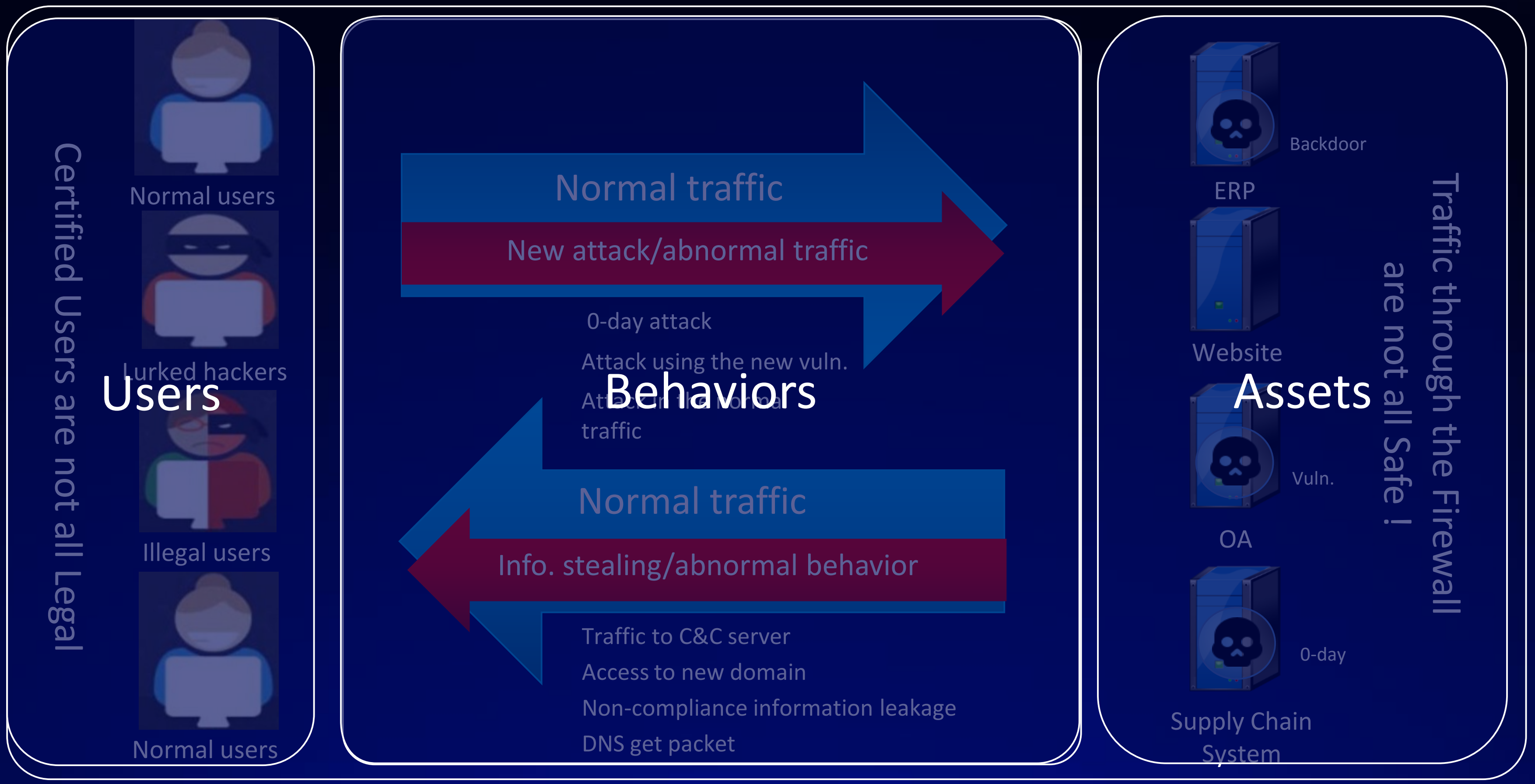
L7 High-Performance

- Hardware and software architecture
- Efficient algorithm

Visibility is the Foundation

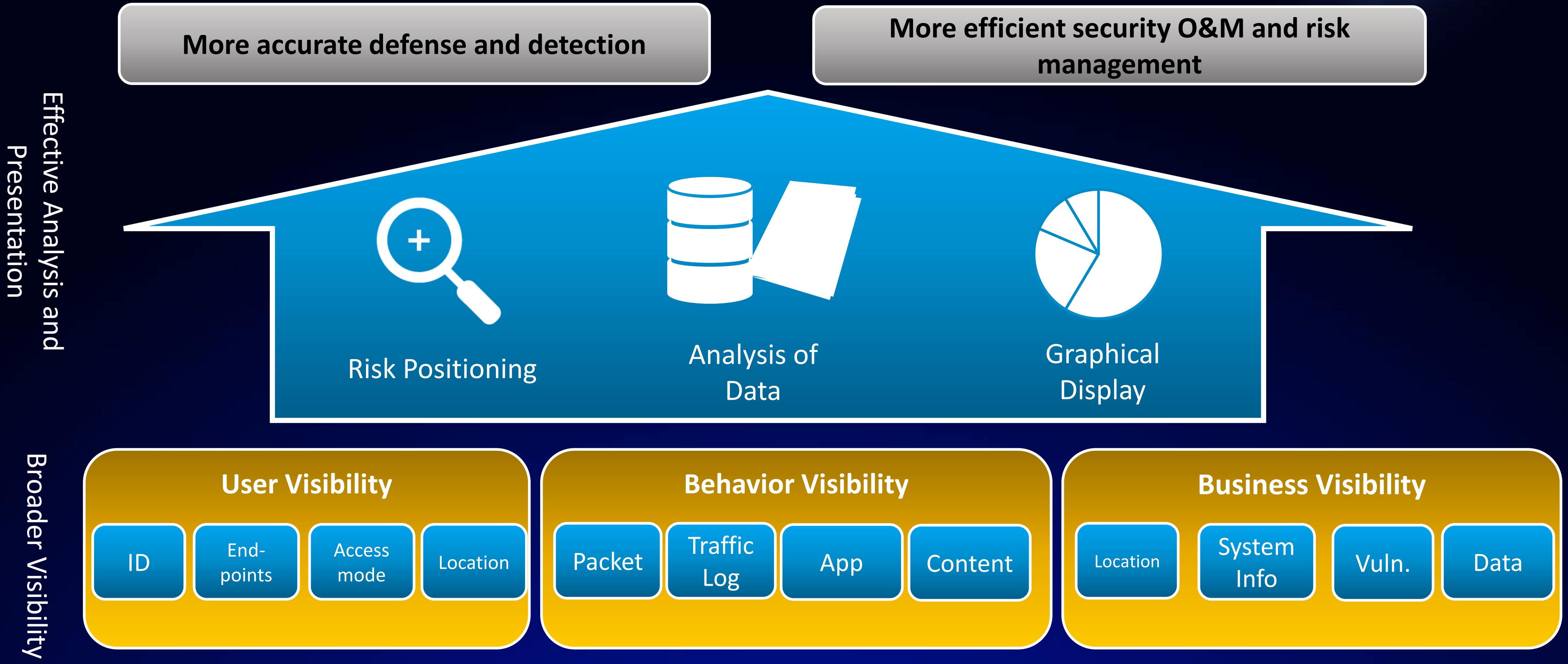
SANGFOR

Many Invisible Security Risk in the Network

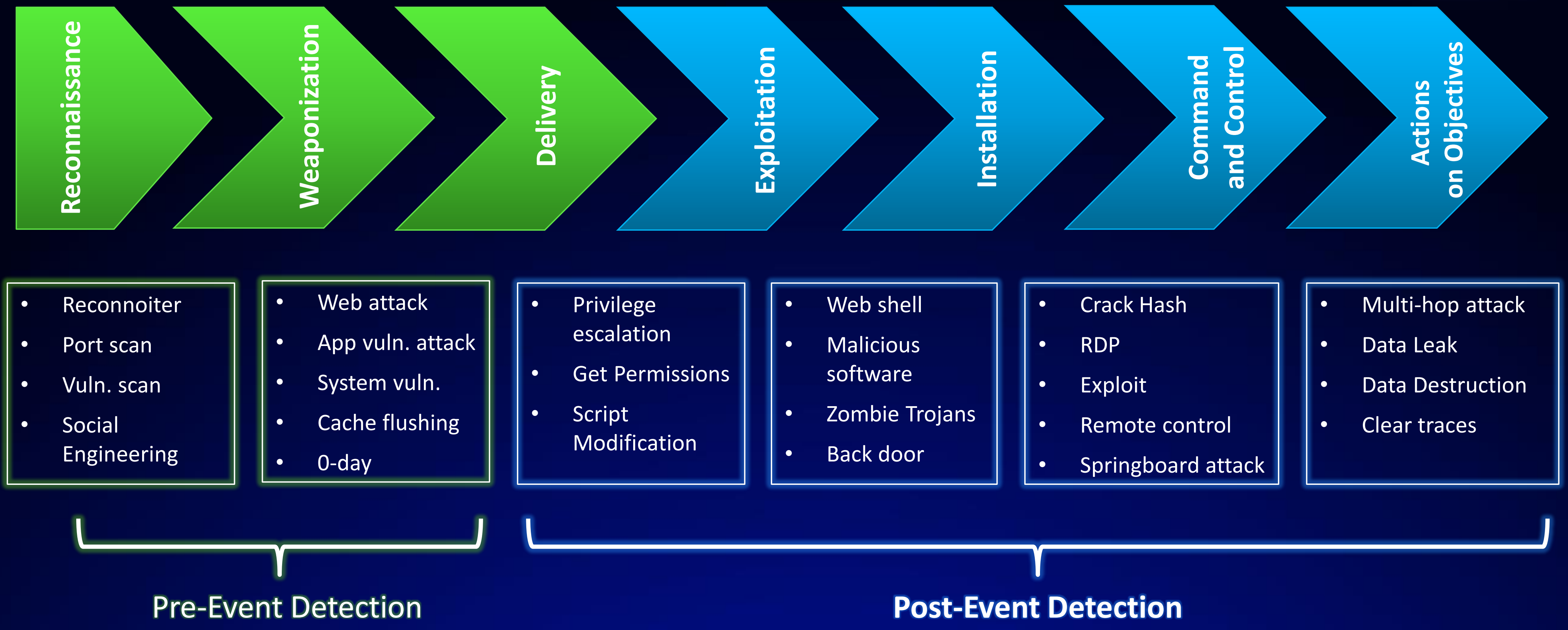

Certified Users are not all Legal
Normal users
Lurked hackers
Users
Illegal users
Normal users
Normal traffic
New attack/abnormal traffic
0-day attack
Attack using the new vuln.
Behaviors
Attack in the normal traffic
Normal traffic
Info. stealing/abnormal behavior
Traffic to C&C server
Access to new domain
Non-compliance information leakage
DNS get packet
Backdoor
ERP
Website
Assets
Vuln.
OA
0-day
Supply Chain System
Traffic through the Firewall are not all Safe !

Not only IP/Port/Signature Visibility, but also Users, Behaviors, Assets and their Correlation !

Broader Visibility and Correlation Analysis



Real-Time Attack Detection Process



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

- Reconnoiter
- Port scan
- Vuln. scan
- Social Engineering

- Web attack
- App vuln. attack
- System vuln.
- Cache flushing
- 0-day

- Privilege escalation
- Get Permissions
- Script Modification

- Web shell
- Malicious software
- Zombie Trojans
- Back door

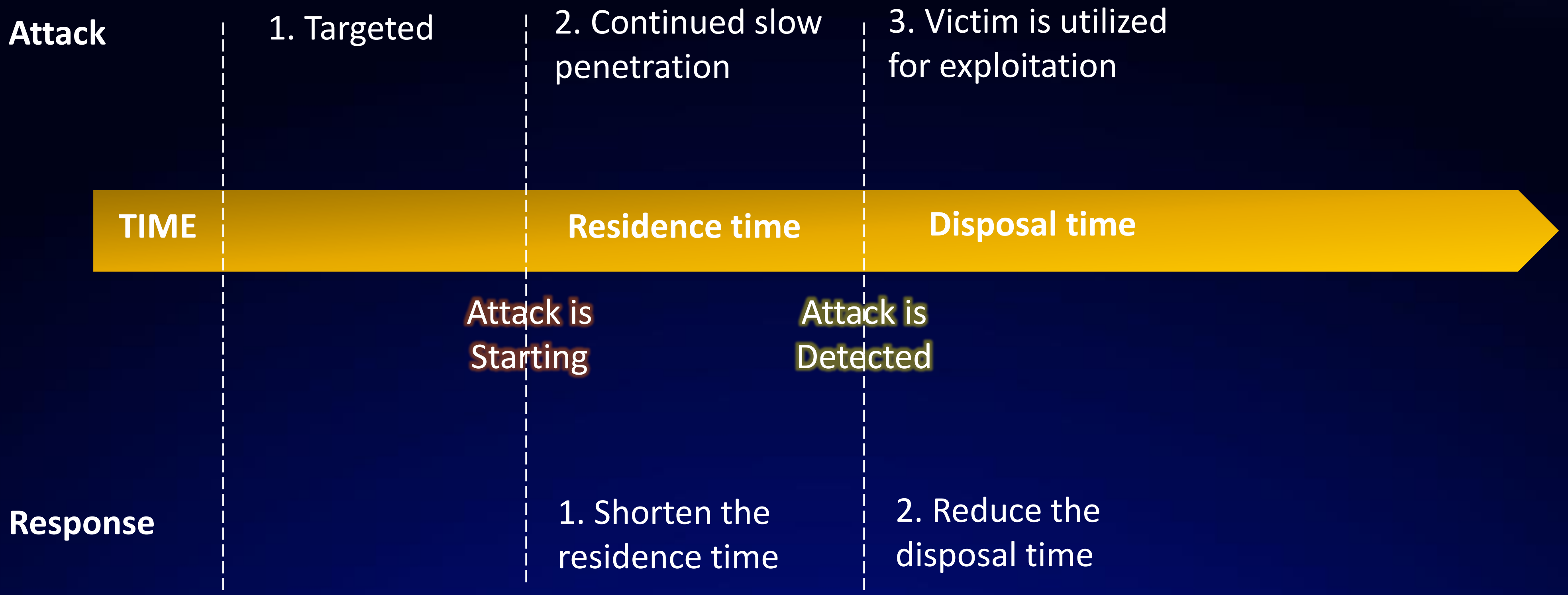
- Crack Hash
- RDP
- Exploit
- Remote control
- Springboard attack

- Multi-hop attack
- Data Leak
- Data Destruction
- Clear traces

Pre-Event Detection

Post-Event Detection

Shorten Detection and Response Time



Attack

1. Targeted

2. Continued slow penetration

3. Victim is utilized for exploitation

TIME

Residence time

Disposal time

Attack is Starting

Attack is Detected

Response

1. Shorten the residence time

2. Reduce the disposal time

Rapid Response: Minimize the loss of security risk, reduce the risk of information assets theft !

Simple Security Operation

Simplified Security

Easy Deployment

configuration wizard

straightforward policy layout

Simple O&M

Intuitive security reporting

Presented as security event

Convergence

- Using wizard to make security deployment simply
- Policy layout: Easily to add rules to the system
- Before system online, check security real time, make sure the system has no vuln., no virus, etc.
- Present vuln. and risks by graghic.
- Security event push, automatic detect, automatic update DB, security advice.
- FW+IPS+AV+WAF integrated

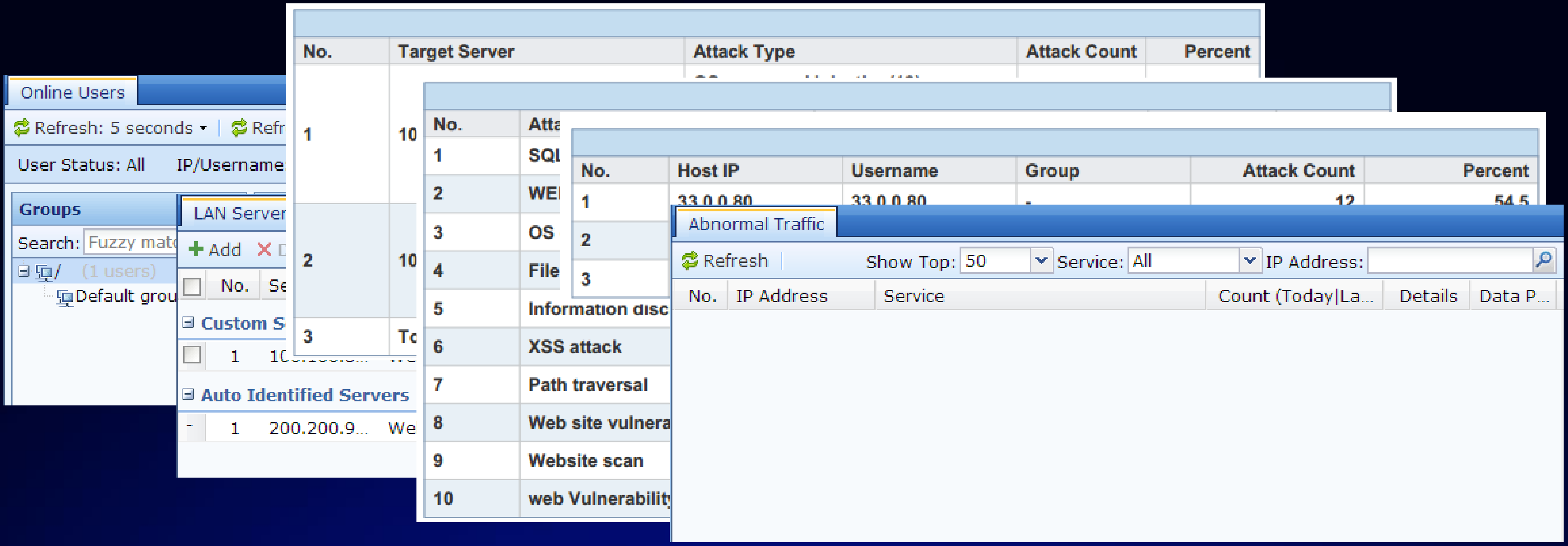
L7 Security High Performance

- **Detection**: Signature, Behavior, Data Analyzing, Machine Learning & Modeling.
- **Software**: Parallel Processing & One-Time Detection.
- **Engine**: High-Performance Patented REGEX Engine.
- **Hardware:** Rich Compute Power.

Table of Content

- Security Trend
- SANGFOR Security Concept
- **NGAF – Your Security Guard to the Future**

Key Elements Visibility



Online Users

Refresh: 5 seconds ▾ | Refr

User Status: All IP/Username

Groups

Search: Fuzzy matc

⊟ / (1 users)

Default grou

LAN Server

+ Add ✕ D

□	No.	Se

⊟ Custom S

□	1	10

⊟ Auto Identified Servers

-	1	200.200.9...	We

No.	Target Server	Attack Type	Attack Count	Percent
1	10			
2	10			
3	To			

No.	Atta
1	SQL
2	WEI
3	OS
4	File
5	Information disc
6	XSS attack
7	Path traversal
8	Web site vulnera
9	Website scan
10	web Vulnerability

No.	Host IP	Username	Group	Attack Count	Percent
1	33.0.0.80	33.0.0.80	-	12	54.5
2					
3					

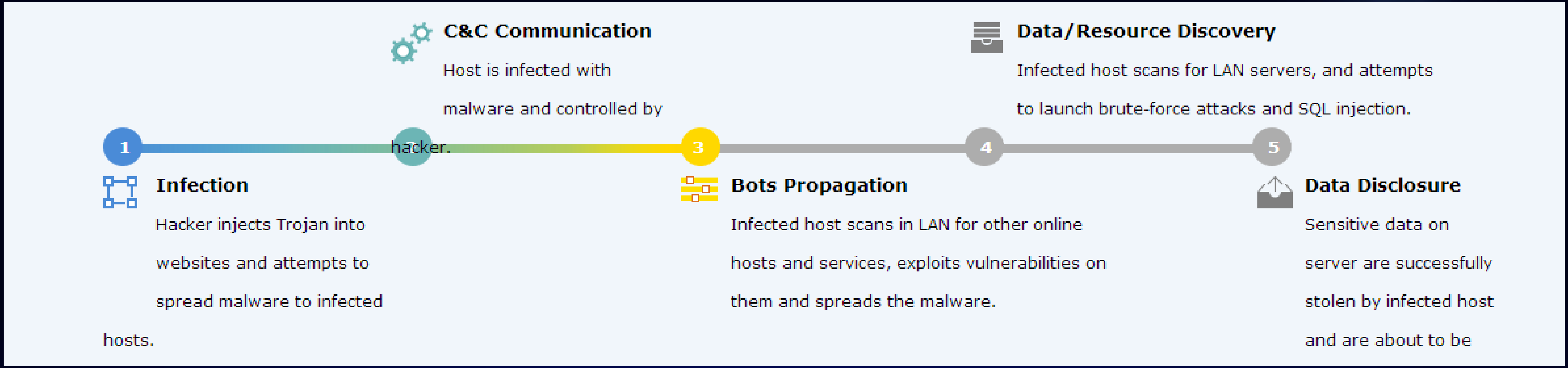
Abnormal Traffic

Refresh | Show Top: 50 Service: All IP Address:

No.	IP Address	Service	Count (Today|La...	Details	Data P...

Attack Status Visibility

SANGFOR



Infection

Hacker injects Trojan into websites and attempts to spread malware to infected hosts.

C&C Communication

Host is infected with malware and controlled by hacker.

Bots Propagation

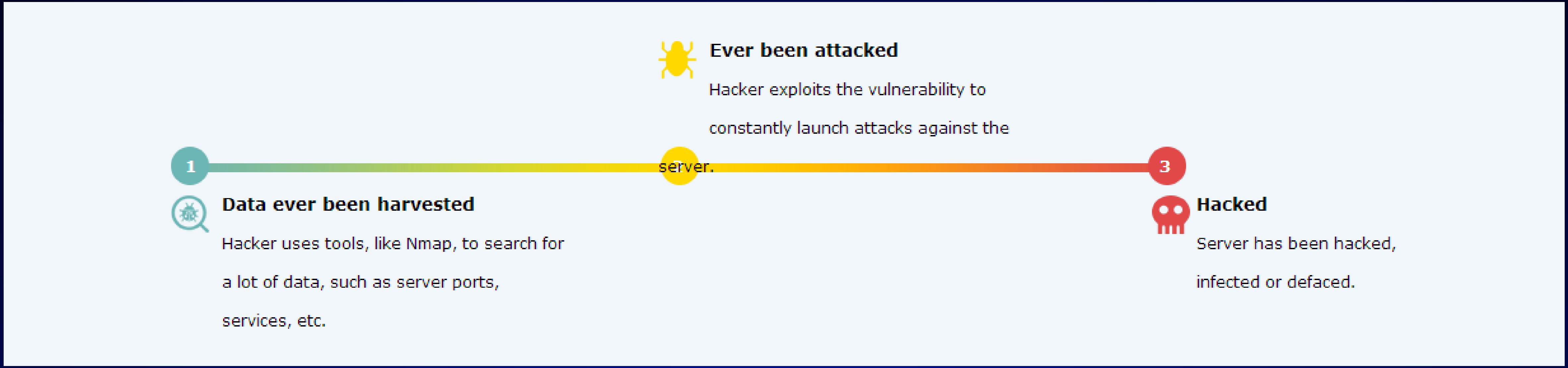
Infected host scans in LAN for other online hosts and services, exploits vulnerabilities on them and spreads the malware.

Data/Resource Discovery

Infected host scans for LAN servers, and attempts to launch brute-force attacks and SQL injection.

Data Disclosure

Sensitive data on server are successfully stolen by infected host and are about to be



Data ever been harvested

Hacker uses tools, like Nmap, to search for a lot of data, such as server ports, services, etc.

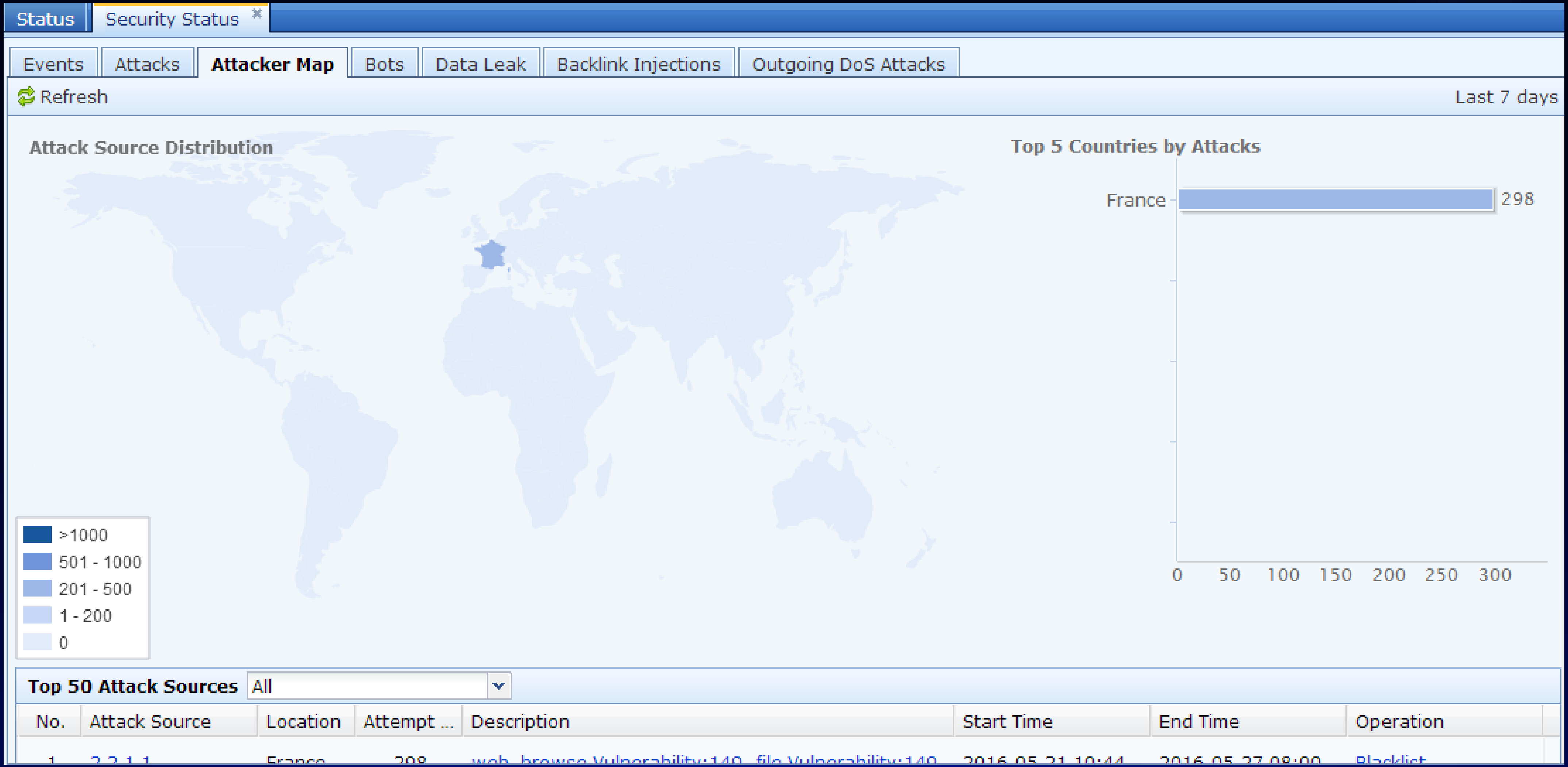
Ever been attacked

Hacker exploits the vulnerability to constantly launch attacks against the server.

Hacked

Server has been hacked, infected or defaced.

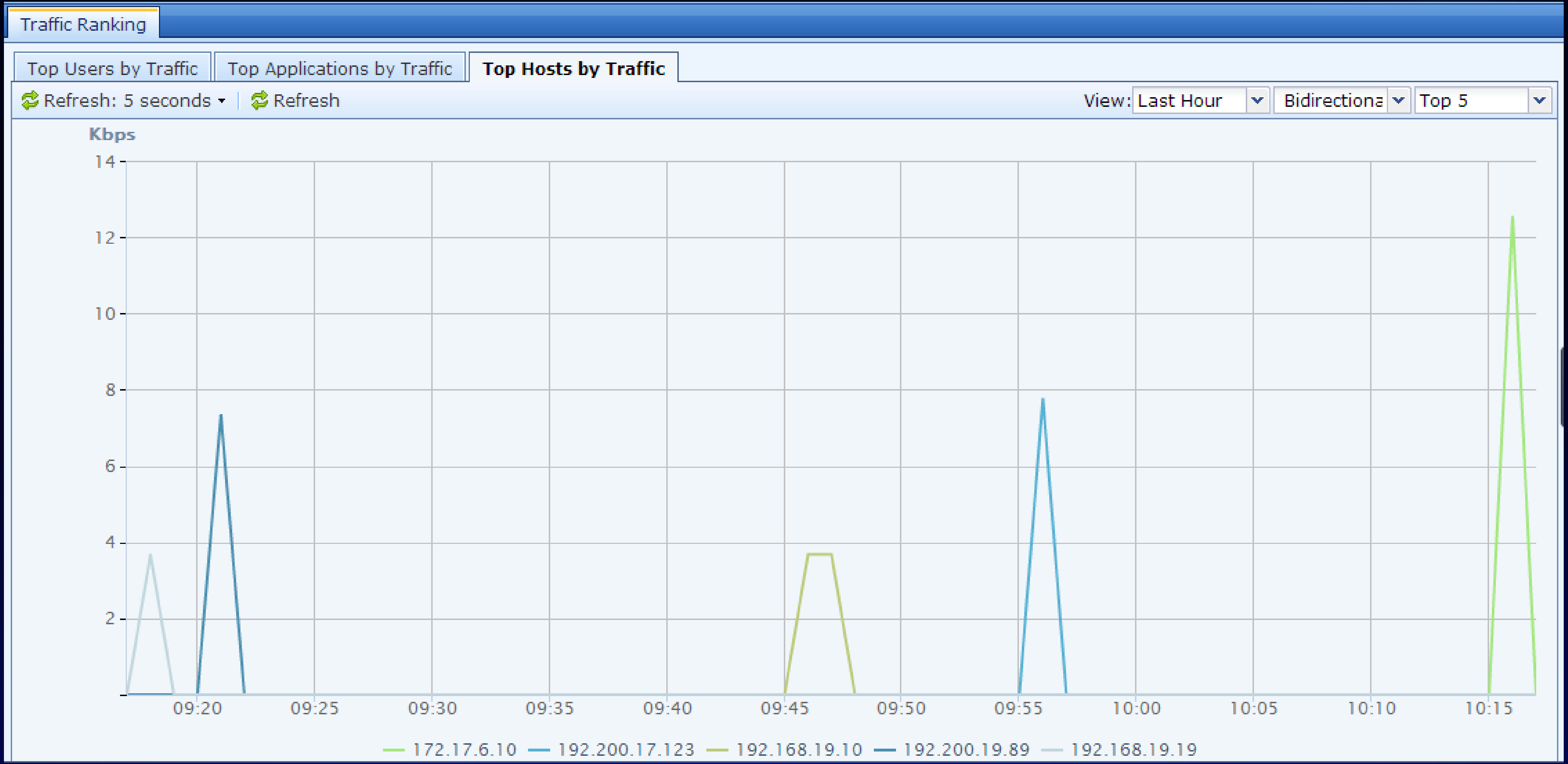
Attack Source Visibility



Top 50 Attack Sources All

No.	Attack Source	Location	Attempt ...	Description	Start Time	End Time	Operation
1	2.2.1.1	France	298	web_browse Vulnerability:149, file Vulnerability:149	2016-05-21 10:44	2016-05-27 08:00	Blacklist

User Traffic Visibility



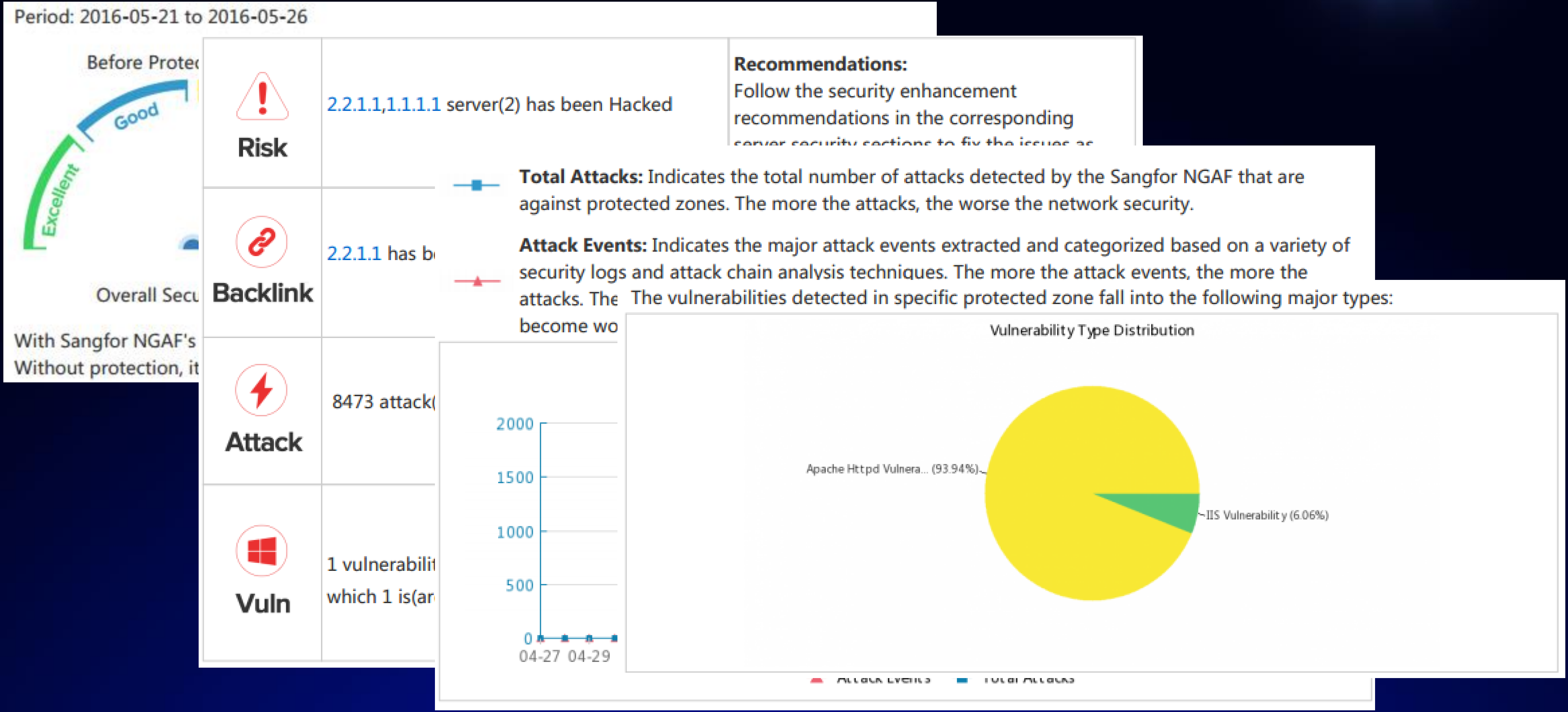
Refresh: 5 seconds

View: Last Hour

Bidirectiona

Top 5

Risk Visibility



Period: 2016-05-21 to 2016-05-26

Before Protec

Overall Secu

With Sangfor NGAF's
Without protection, it

Risk	2.2.1.1,1.1.1.1 server(2) has been Hacked	**Recommendations:** Follow the security enhancement recommendations in the corresponding server security sections to fix the issues as
Backlink	2.2.1.1 has b	
Attack	8473 attack(	
Vuln	1 vulnerabilit which 1 is(ar	

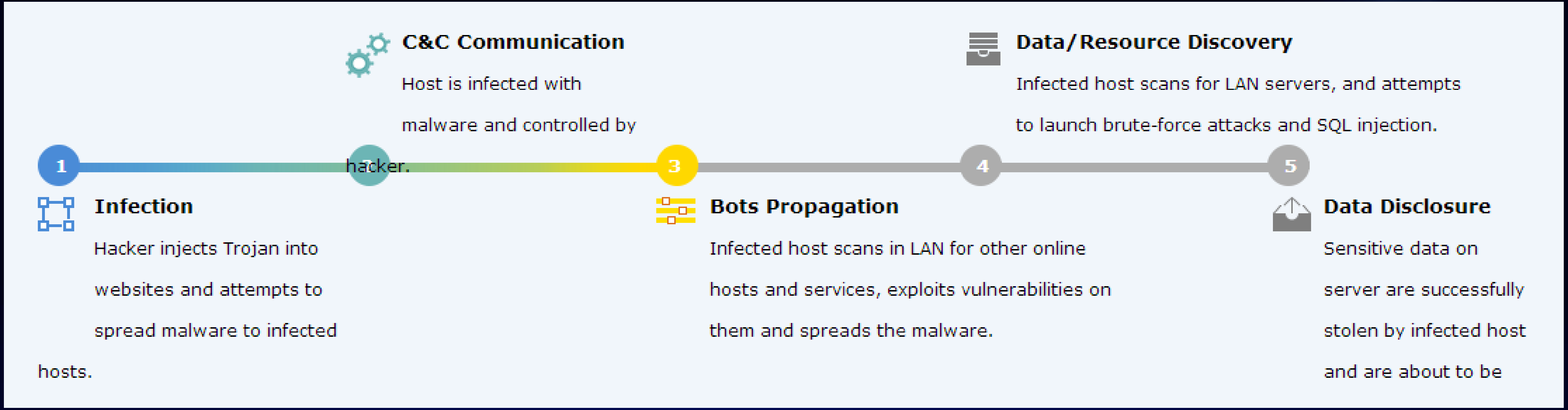
Total Attacks: Indicates the total number of attacks detected by the Sangfor NGAF that are against protected zones. The more the attacks, the worse the network security.

Attack Events: Indicates the major attack events extracted and categorized based on a variety of security logs and attack chain analysis techniques. The more the attack events, the more the attacks. The become wo

The vulnerabilities detected in specific protected zone fall into the following major types:

Vulnerability Type Distribution

All Risk Real-Time Detection of Attack Process



Infection

Hacker injects Trojan into websites and attempts to spread malware to infected hosts.

C&C Communication

Host is infected with malware and controlled by hacker.

Bots Propagation

Infected host scans in LAN for other online hosts and services, exploits vulnerabilities on them and spreads the malware.

Data/Resource Discovery

Infected host scans for LAN servers, and attempts to launch brute-force attacks and SQL injection.

Data Disclosure

Sensitive data on server are successfully stolen by infected host and are about to be

Detection Technology

- Email AV
- Cloud AV(Multi-engine)
- Cloud sandbox
- Malicious trojan detection
- Attack feature detection

- Malicious link detection(auto)
- Trojan remote control detection
- Abnormal traffic detection
- Anomaly protocol on standard port detection

- LAN attack detection
- Internal scanning behavior detection
- Illegal access detection
- Password cracking behavior detection
- Virus transmission detection

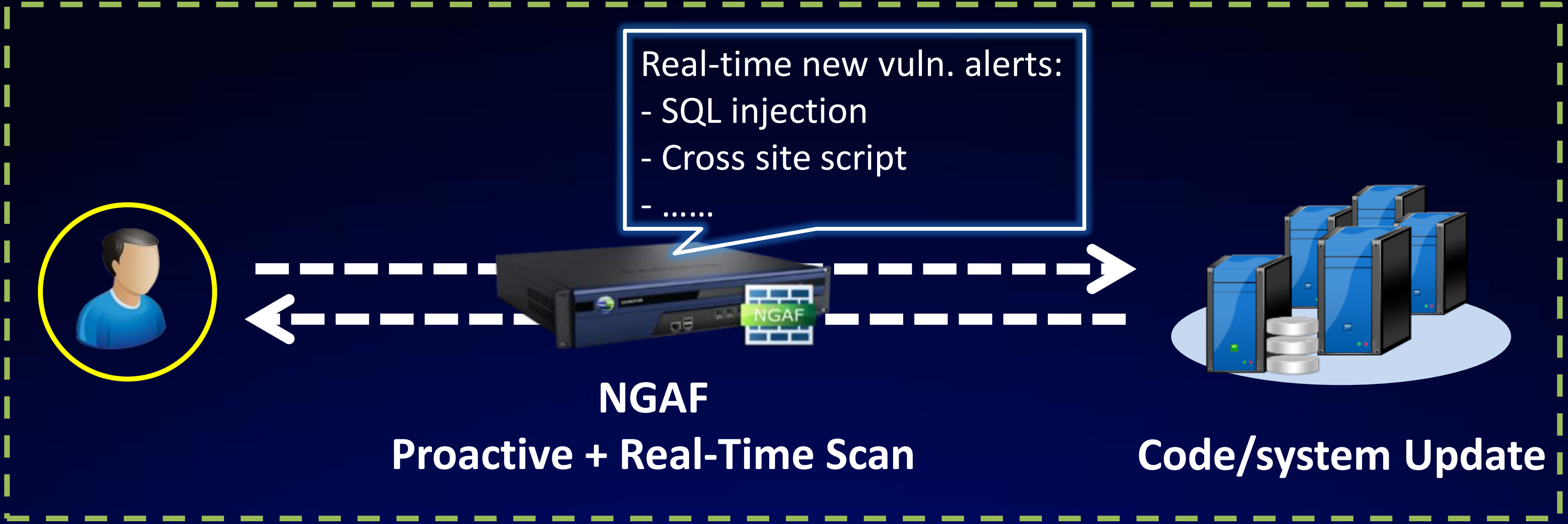
- Real-time vuln. detection
- Web app vuln. detection
- Web attack detection
- Web shell detection

- Data leakage detection
- Backdoor using detection
- Ramsomware detection
- Web page tampering detection
- Back link detection

Hundreds of Abnormal Behavior and Threat Detection Technologies

Real-Time Detection of Business System Vulnerabilities

Assets = Business   Threat = Attack   Vulnerability = Loophole



Real-time new vuln. alerts:
- SQL injection
- Cross site script
- ……

NGAF
Proactive + Real-Time Scan

Code/system Update

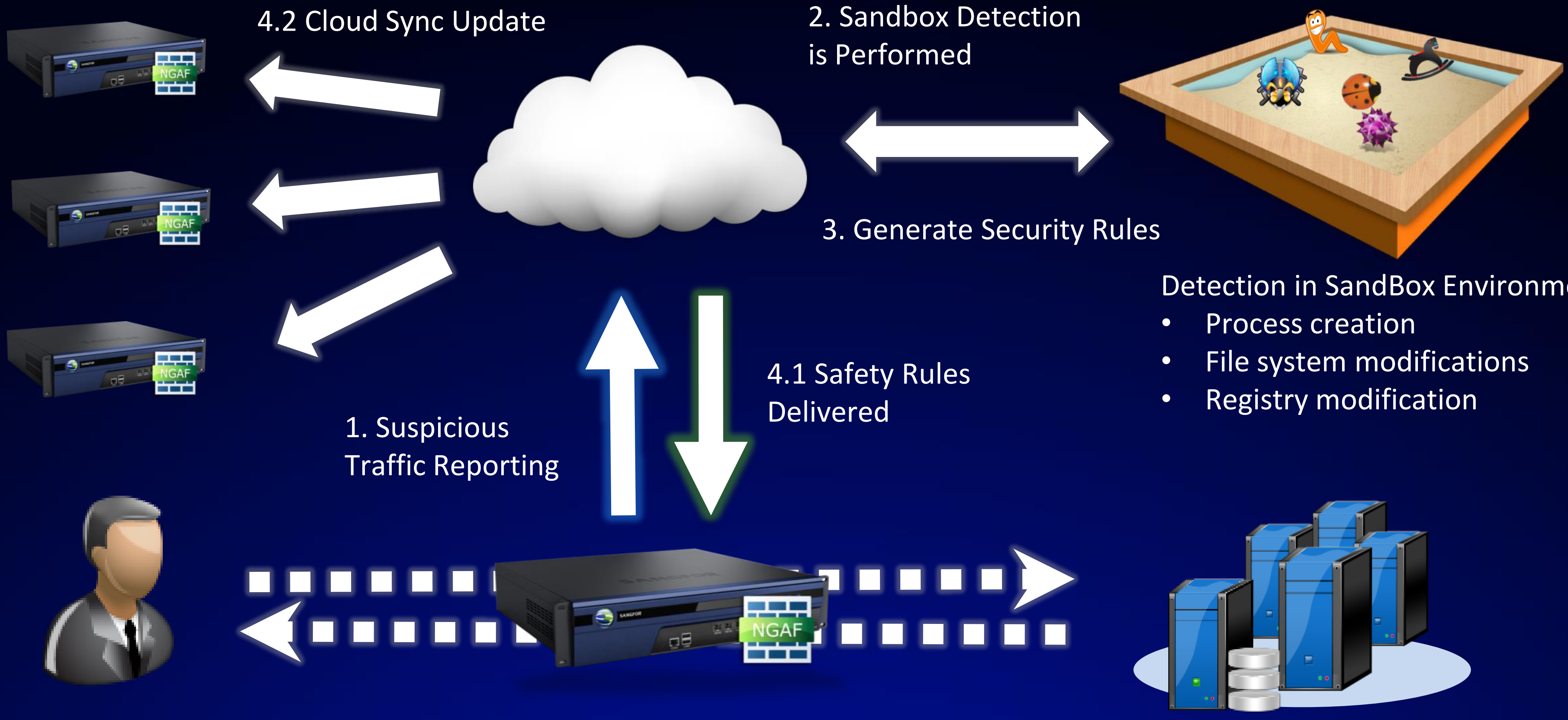
Threats Recognition

Vuln. Recognition

Assets Recognition

Provide Active & Passive Vulnerability Detection, 7*24-hour Vulnerability Monitoring Service

Unknown Threats Detection - Sangfor Cloud Sandbox



1. Suspicious Traffic Reporting

2. Sandbox Detection is Performed

3. Generate Security Rules

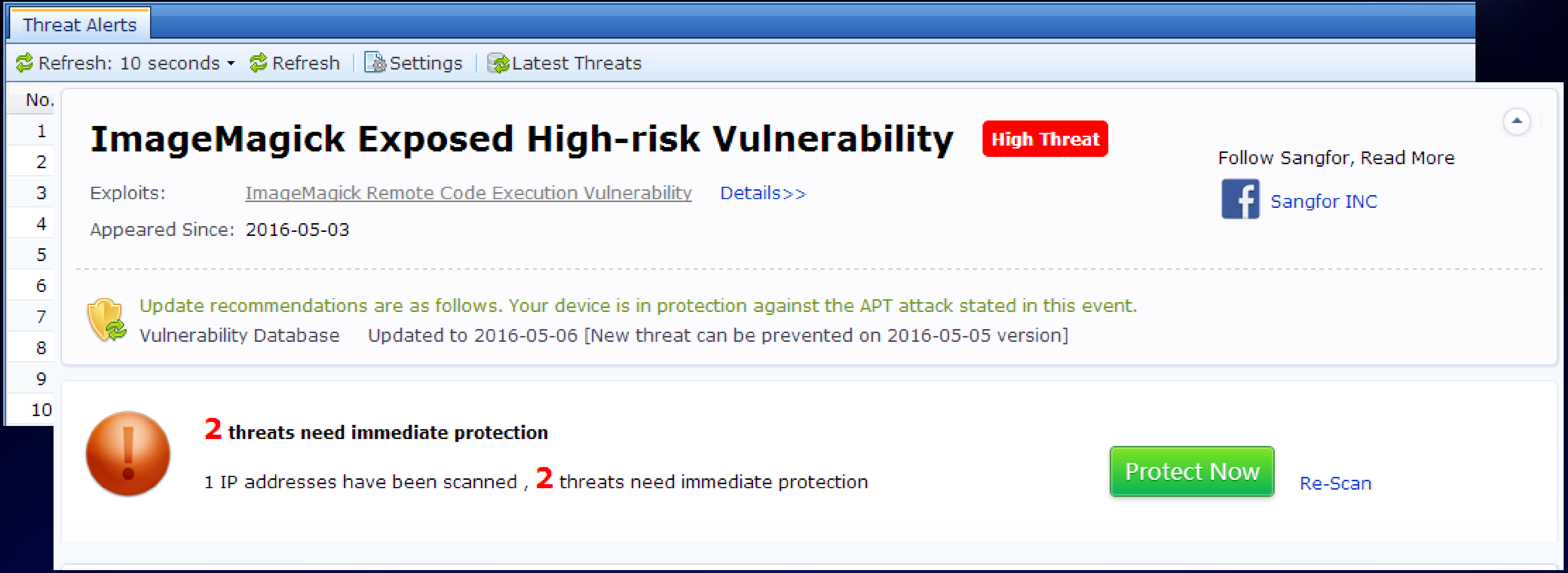
4.1 Safety Rules Delivered

4.2 Cloud Sync Update

Detection in SandBox Environment:

- Process creation
- File system modifications
- Registry modification

Rapid Response to New Threats



ImageMagick Exposed High-risk Vulnerability

High Threat

Exploits: ImageMagick Remote Code Execution Vulnerability Details>>

Appeared Since: 2016-05-03

Follow Sangfor, Read More

Sangfor INC

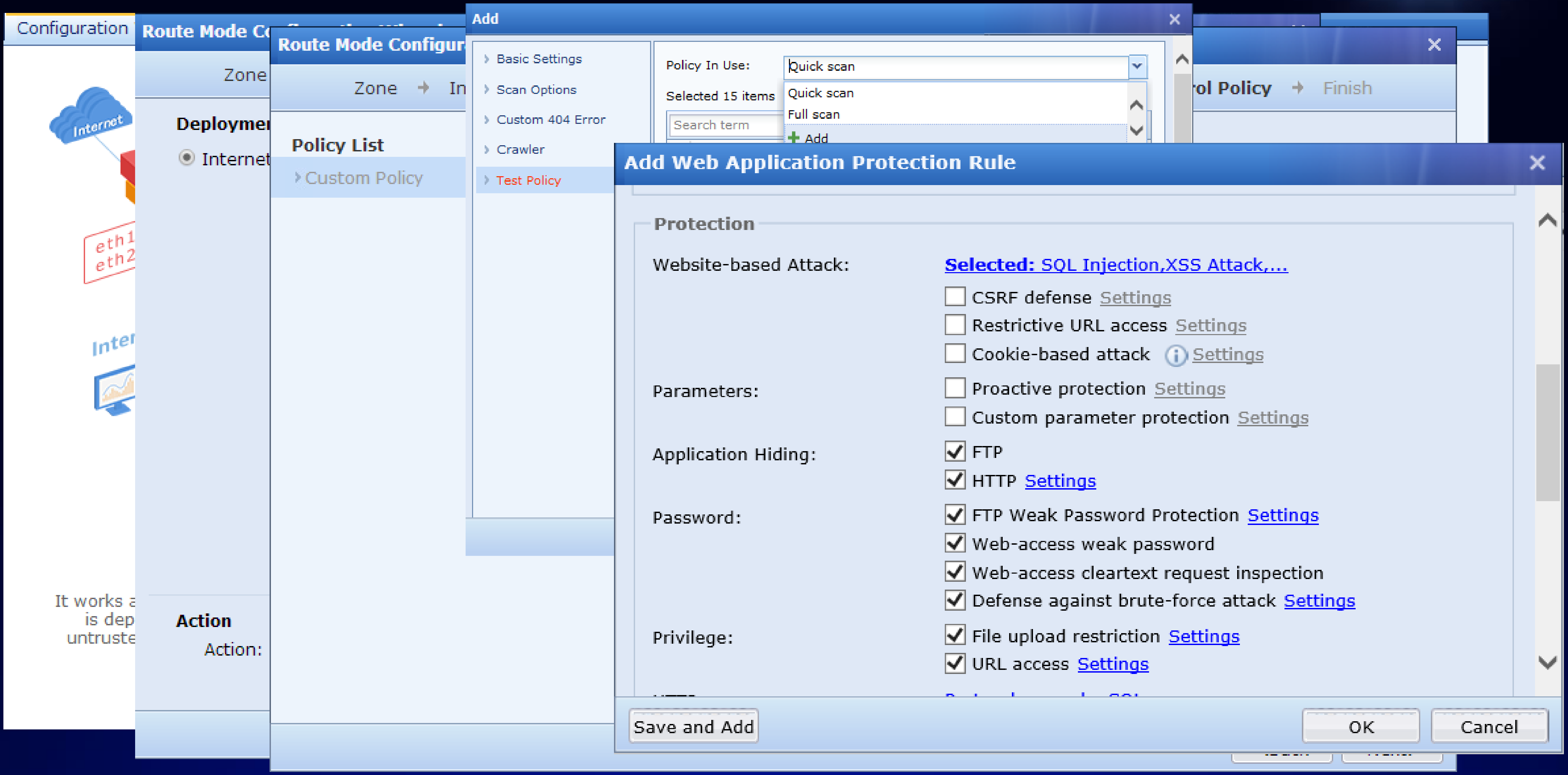
Update recommendations are as follows. Your device is in protection against the APT attack stated in this event.

Vulnerability Database Updated to 2016-05-06 [New threat can be prevented on 2016-05-05 version]

2 threats need immediate protection

1 IP addresses have been scanned , 2 threats need immediate protection

Configuration Wizard/Policy Layout



Policy In Use: Quick scan

Selected 15 items

Add Web Application Protection Rule

Protection

Website-based Attack: Selected: SQL Injection,XSS Attack,...

□ CSRF defense Settings

□ Restrictive URL access Settings

□ Cookie-based attack Settings

Parameters:

□ Proactive protection Settings

□ Custom parameter protection Settings

Application Hiding:

☑ FTP

☑ HTTP Settings

Password:

☑ FTP Weak Password Protection Settings

☑ Web-access weak password

☑ Web-access cleartext request inspection

☑ Defense against brute-force attack Settings

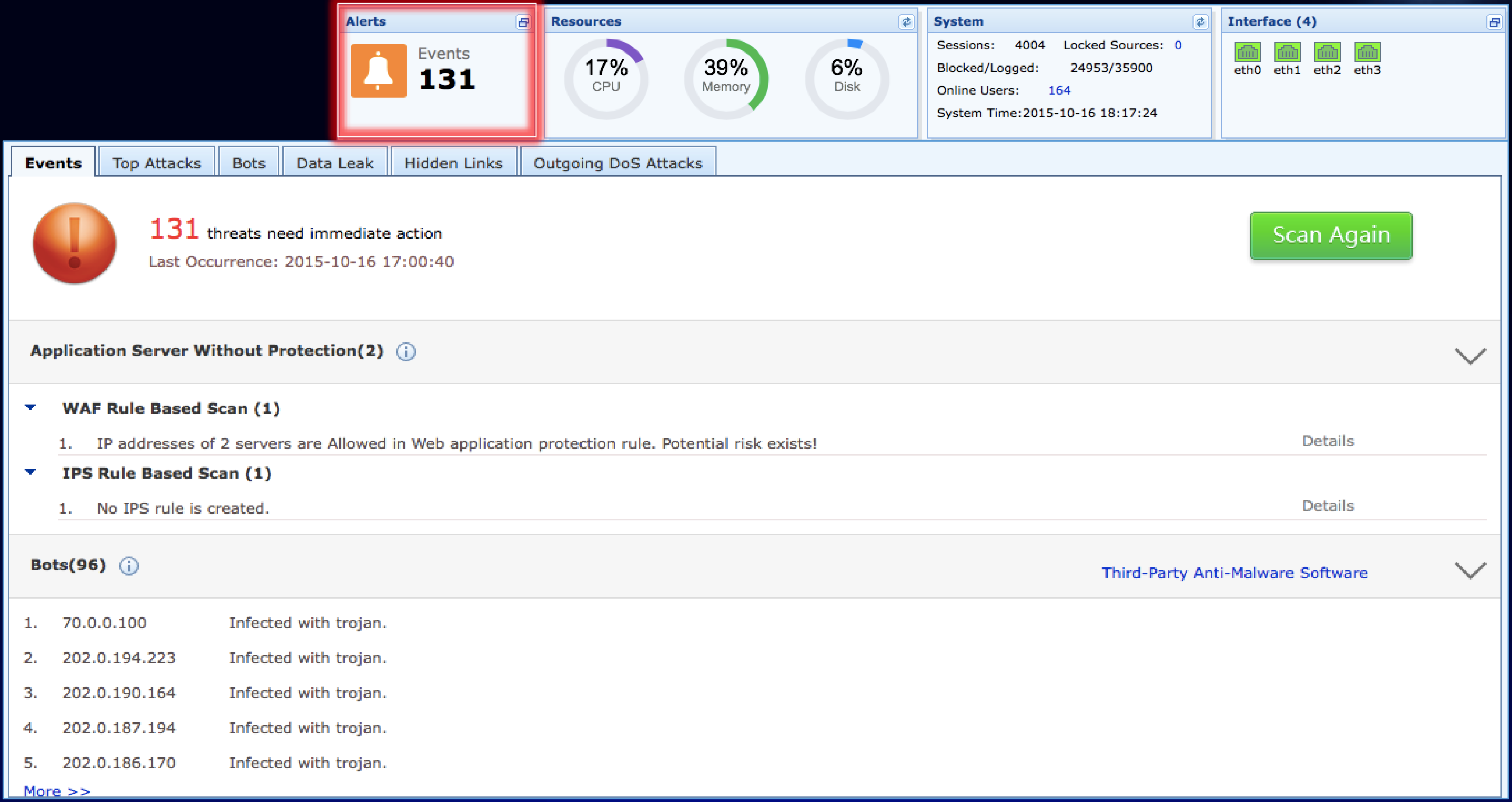
Privilege:

☑ File upload restriction Settings

☑ URL access Settings

Automated Security Operation Guidance

SANGFOR



Alerts

Events 131

Resources

17% CPU

39% Memory

6% Disk

System

Sessions: 4004 Locked Sources: 0

Blocked/Logged: 24953/35900

Online Users: 164

System Time:2015-10-16 18:17:24

Interface (4)

131 threats need immediate action

Last Occurrence: 2015-10-16 17:00:40

Application Server Without Protection(2)

WAF Rule Based Scan (1)

1. IP addresses of 2 servers are Allowed in Web application protection rule. Potential risk exists! Details

IPS Rule Based Scan (1)

1. No IPS rule is created. Details

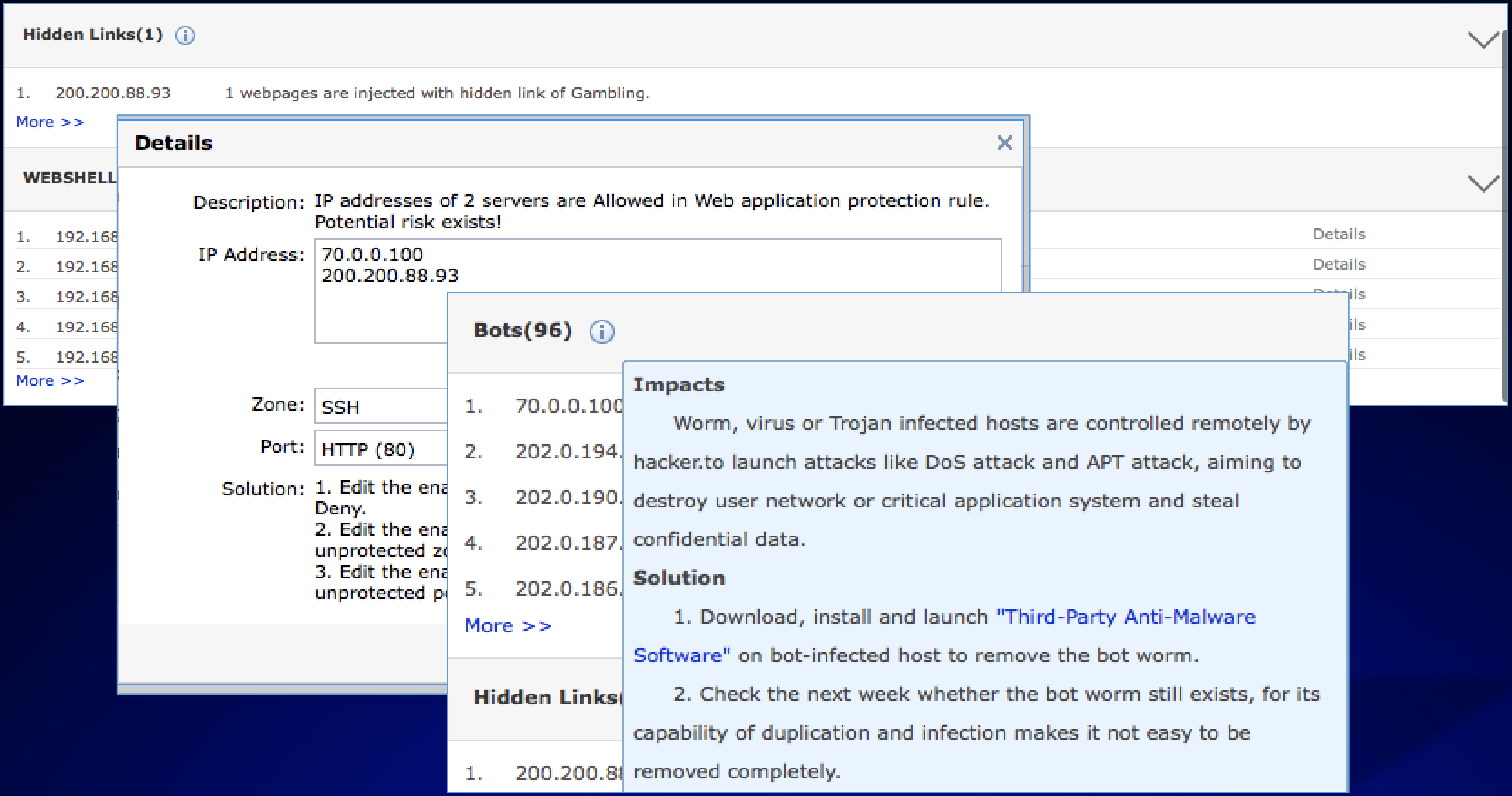
Bots(96)

Third-Party Anti-Malware Software

1. 70.0.0.100 Infected with trojan.
2. 202.0.194.223 Infected with trojan.
3. 202.0.190.164 Infected with trojan.
4. 202.0.187.194 Infected with trojan.
5. 202.0.186.170 Infected with trojan.

More >>

Automated Security Operation Guidance



Hidden Links(1)

1. 200.200.88.93 1 webpages are injected with hidden link of Gambling.

More >>

WEBSHELL

1. 192.168

2. 192.168

3. 192.168

4. 192.168

5. 192.168

More >>

Details

Description: IP addresses of 2 servers are Allowed in Web application protection rule. Potential risk exists!

IP Address: 70.0.0.100
200.200.88.93

Zone: SSH

Port: HTTP (80)

Solution: 1. Edit the ena
Deny.
2. Edit the ena
unprotected zo
3. Edit the ena
unprotected p

Bots(96)

1. 70.0.0.100

2. 202.0.194.

3. 202.0.190.

4. 202.0.187.

5. 202.0.186.

More >>

Hidden Links

1. 200.200.8

Impacts

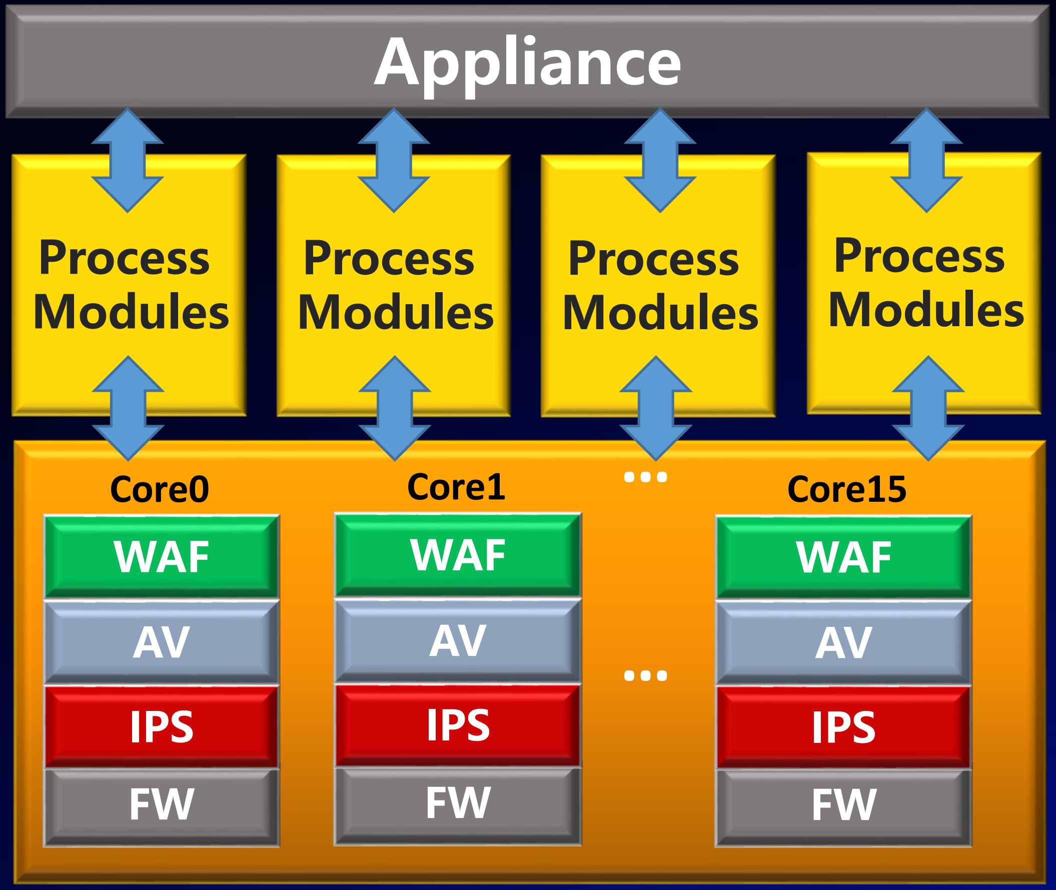
Worm, virus or Trojan infected hosts are controlled remotely by hacker.to launch attacks like DoS attack and APT attack, aiming to destroy user network or critical application system and steal confidential data.

Solution

1. Download, install and launch "Third-Party Anti-Malware Software" on bot-infected host to remove the bot worm.

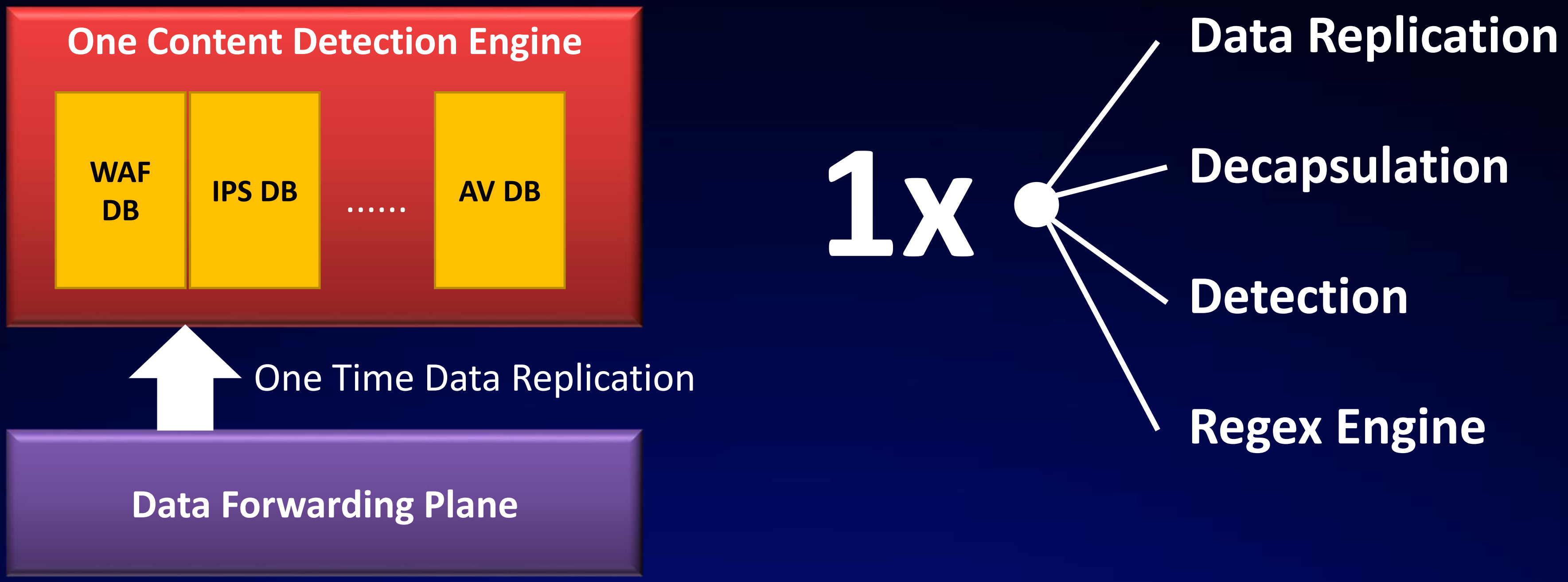
2. Check the next week whether the bot worm still exists, for its capability of duplication and infection makes it not easy to be removed completely.

SANGFOR NGAF Hardware Architecture



- **Intel Quick Path Interconnect**
  - Wide bus bandwidth
  - High computing capacity
- **Multi-Core Level Processing**
  - Up to 2.5GHz
  - Up to 126 cores
- **Hybrid Processing Model**
  - Fragmentated processing
  - One module can use all power

SANGFOR NGAF Software Architecture



One Content Detection Engine

WAF DB

IPS DB

……

AV DB

One Time Data Replication

Data Forwarding Plane

1x

Data Replication

Decapsulation

Detection

Regex Engine

Low latency

High throughput

Good flexibility

High performace

Conclusion

New Business Environment Drives New Security Model !

- **Real Time Security Visibility** is the foundation of modern security.

- **Fast response** to security events is crucial.

- Security **operation simplification** becomes part of security requirements.

- **Application layer Security** capability is what new security cares about.

Thank you !

Global Service Center:
+60 12711 7129 (7511)

sales@sangfor.com
marketing@sangfor.com

Your Security Guard to the Future