SANGFOR

Sangfor Next Generation Application Firewall

Sangfor security team

Agenda

1 PART
Introduction

2 PART
Sangfor NGAF

3 PART
Integrated Network & Endpoint

4 PART
Competitive Landscape

5 PART
Sangfor NGAF reputation

PART 1 Introduction

Evolving Threat In Digital Economy Era

ATP, Ransomware. Data breaches,

and the list goes on

Ransomware
>50 Russian company infected

APT
PyeongChang Winter Olympics suffered a phishing email attack causing network downtime

Data Breach
Marriott's 500 million customer data leaked, and its share price fell by 6.9%.

State-sponsored Attack
SingHealth reported an attack compromising the personal information of 1.5 million patients' detail

You Can't Protect If You Can't See

Software Exploits

Application Attacks

Unknown & Exposed Devices

Unknown assets can be attacked

- BYOD
- Print servers

Crypto Ransomware

Unknown Threats

Network and Application Threats

Changes in your network left assets exposed

- Forgotten test servers
- Change in your firewall rules

Stealth Malware

Credential Harvesting

Unknown & Non-Classified Traffic

Average Users are easy target

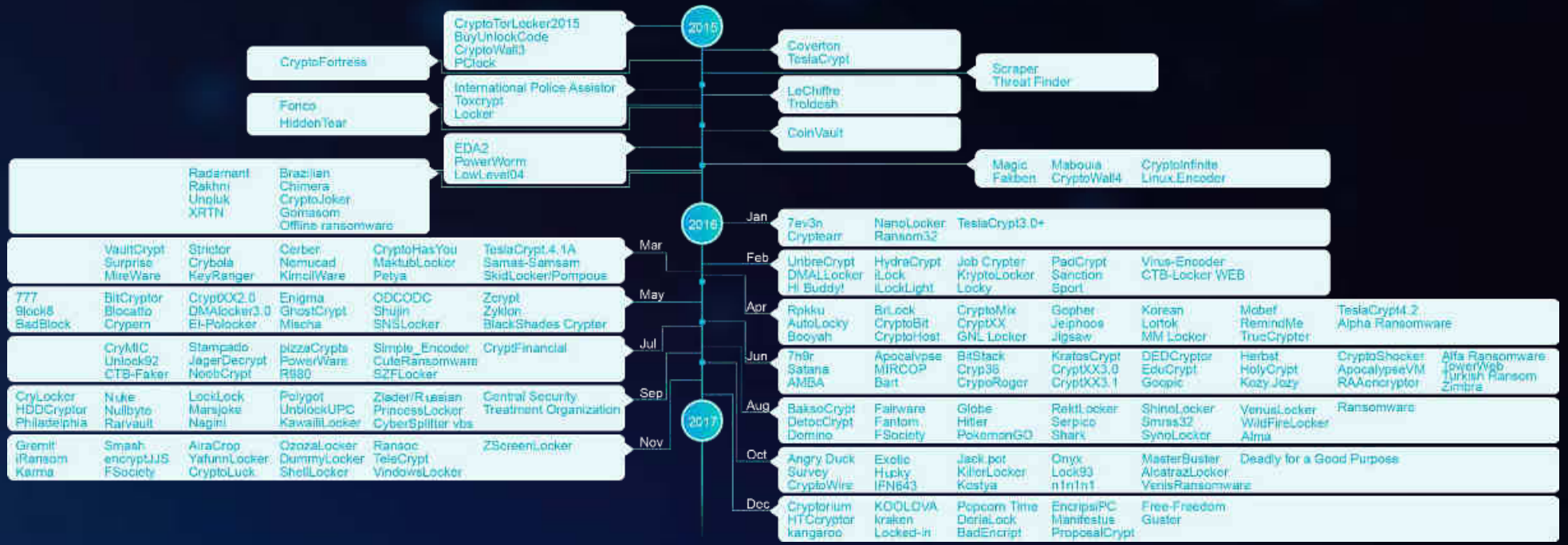
- Phishing emails
- Infected malware

Attacks Bypass Traditional Protection

WannaCry Ransomware infected **200,000** machines in **four days** across **150 countries.**

In a recent Barkly survey of companies who suffered ransomware attacks in the past 12 months:

- **100%** of customers were running anti-virus
- **95%** of attacks bypassed traditional firewall
- **77%** of attacks bypassed email security



Case Study - TSMC Exposed to Ransomware

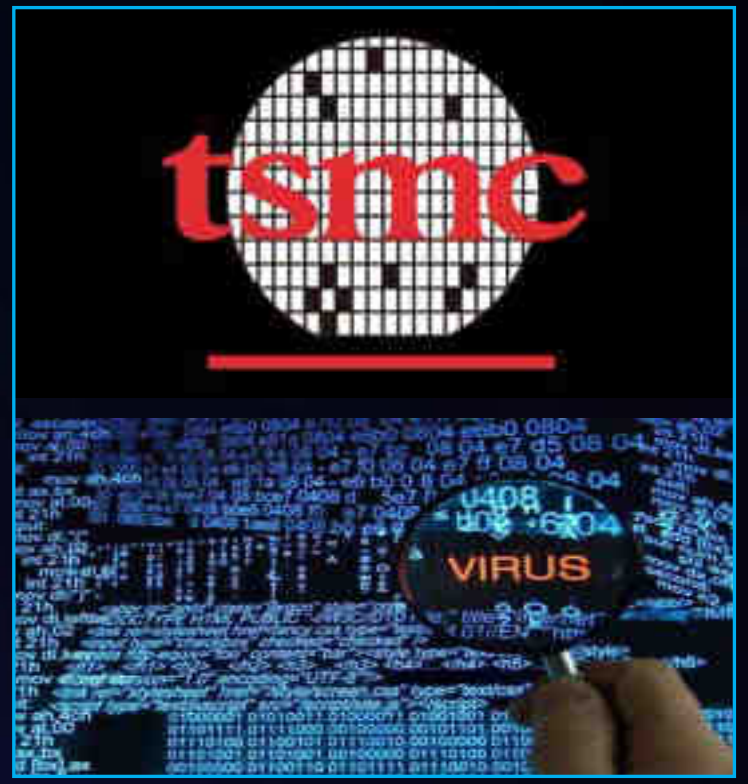
Date & Time: August, 3rd – 6th 2018

Loss: 2.596 billion

Industry: Manufacturing

Event Profile:

- The largest semiconductor company in Taiwan
- Company statement shows the ransomware came from a newly connected computer
- TSMC's stock dropped 15.2% in 3 days
- TSMC announced that luckily, their core codes weren't lost
- Considered the most serious WannaCry attack globally, as of 2018



PART 2 Sangfor NGAF

Sangfor Security Framework

Fully Protected Network, Endpoint & Cloud

Continuous Evolution of Capabilities Using Cloud-Based TI & AI

Correlation, Detection & Response

Security Operations Managed Service

What's NGAF?

SANGFOR

Total threat prevention

- Packet filter
- Stateful
- ACL

Firewall
1990s'

- Signature
- Anomaly
- Heuristic

2000s'

- DPI
- Malware
- Sandboxing

2000s'-2010s'

- Http/Web-based attack
- Automatic policy learning

WAF
2000s'-2010s'

Total Cost of Ownership

Risk mitigation

NGFW+ WAF in one box

Security effectiveness

Offload security operation

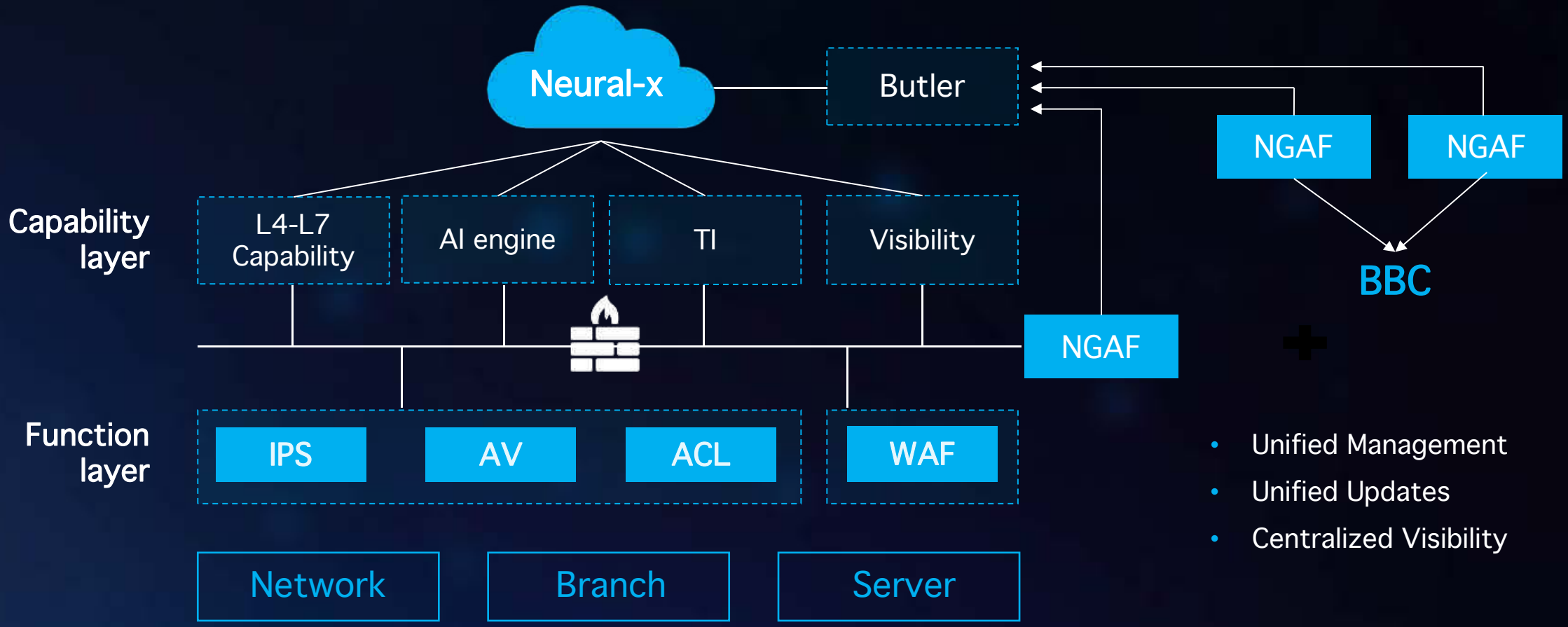
End to End Security Protection in One Box

Comprehensive and Reliable Protection From L2 to L7

The Worlds First AI Enabled NGAF Fully Integrated NGFW + NGWAF + Security visibility

Sangfor NGAF Firewall Capability Architecture

Advantages: Effective & Simple



- Unified Management
- Unified Updates
- Centralized Visibility

Sangfor NGAF Firewall Capability Architecture

SANGFOR

Visibilit y

Neural-X

Engine Zero

NGWAF

Unknown Threats Prevention:

- Converged security
- AI-Based Malware Inspection
- Security Context

Protect Business Assets

- Asset Discovery
- Vulnerability Assessment
- Next Generation WAF

Simplified Security Operation

- Superior Visibility
- Unmatched Reporting
- Expertise Services

Sangfor Engine Zero:
On Premise AI Based Malware Inspection

Deep Learning is Everywhere

Sangfor Engine Zero:
Deep Learning Neural Networks

- Protection from both known and unknown malware
- No reliance on signatures
- Detects malware in approximately 30 milliseconds
- Extremely small footprint (under 60MB)
- Works out of the box. No additional training required

Sangfor Engine Zero:
On Premise AI Based Malware Inspection

Coverage

Both known and zero-day attacks.

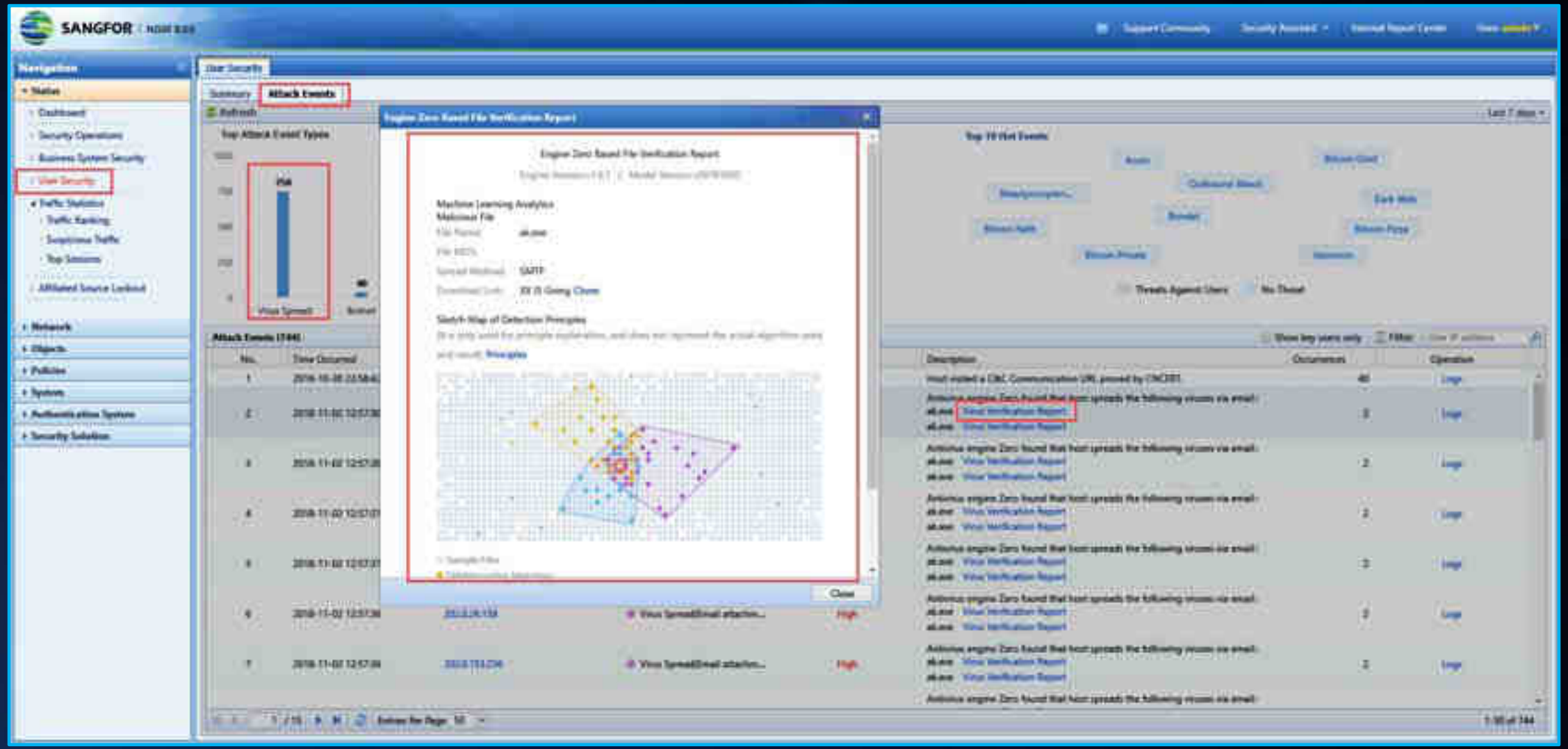
Efficacy

In recent tests our malware detection rate scored the highest in terms of accuracy among other vendors.

Fast

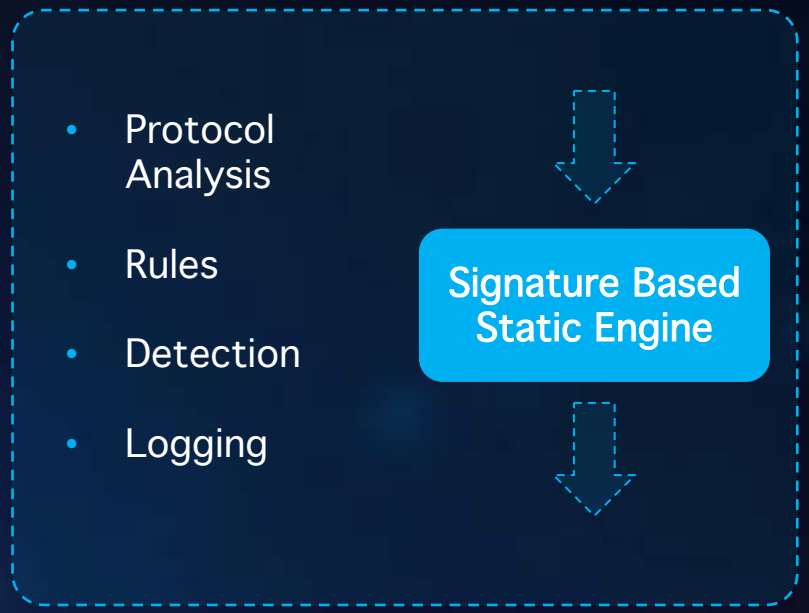
Extremely efficient, utilizing very few resources while efficiently providing malware inspection on the network gateway with very little performance impact.

Sangfor Engine Zero Malware Detection



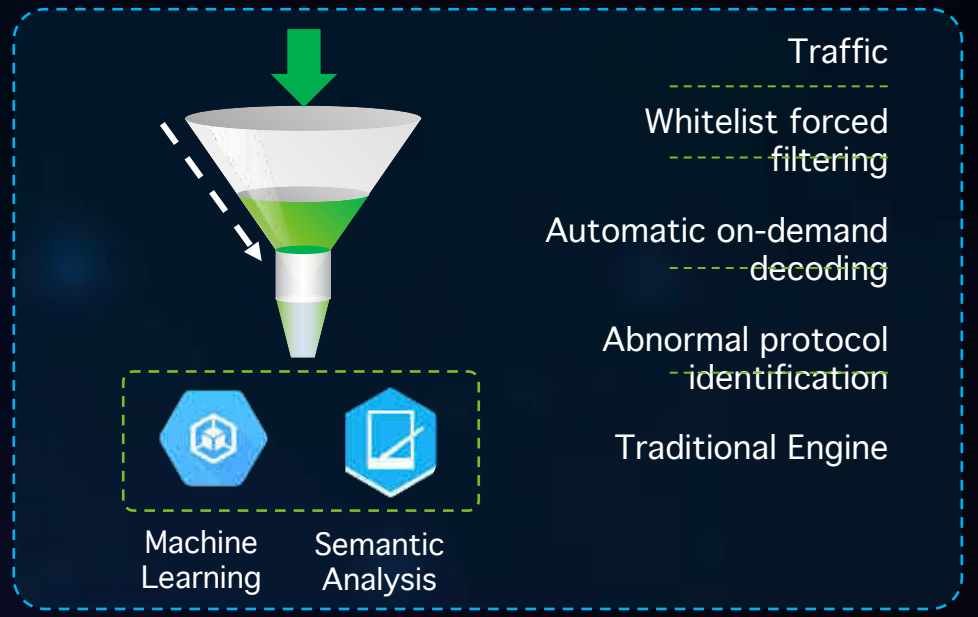
Sangfor Next Generation WAF Engine

Traditional Engine



- Unable to detect unknown threats and exploits
- Easy to bypass
- Common false positive SQL injection detection
- Low-level performance

NGWAF Engine



- Comprehensively surpasses sort rules to identify unknown threats and high-risk vulnerabilities
- Automatically learns by modeling normal business traffic, reducing false positives by 62.4%

Proven Success Protecting Web Applications

OWASP
Open Web Application Security Project

OWASP

Scanning Process

- Prevents port/server scanning
- Prevents app vulnerability scanning
- Weak password protection
- Anti-brute force attack
- Core URL protection
- Website structure anti-scanning
- Web Crawler defense

Attack Process

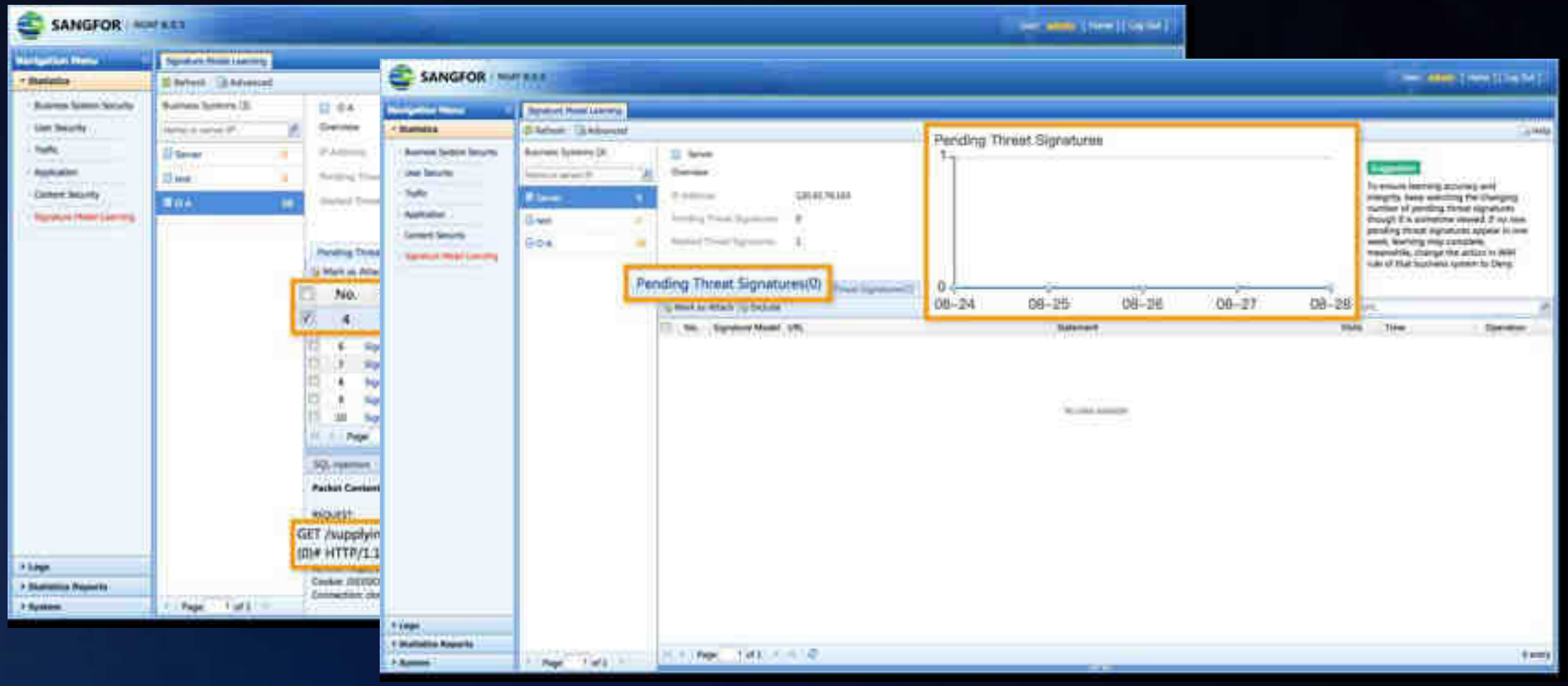
Enhanced Web Defense
- SQL injection defense
- OS command injection defense
- XSS attack & CSRF attack

IPS Application Based
- Server vulnerability defense
- Terminal vulnerability defense

Theft Process

- DOS attack
- Application layer DOS attack
- CC attack
- Authority control
- Exe file upload filtering
- Upload viruses & Trojan filtering
- Prevention of web shell dataflow

Machine Learning for Business Model, Reduce the False Positive

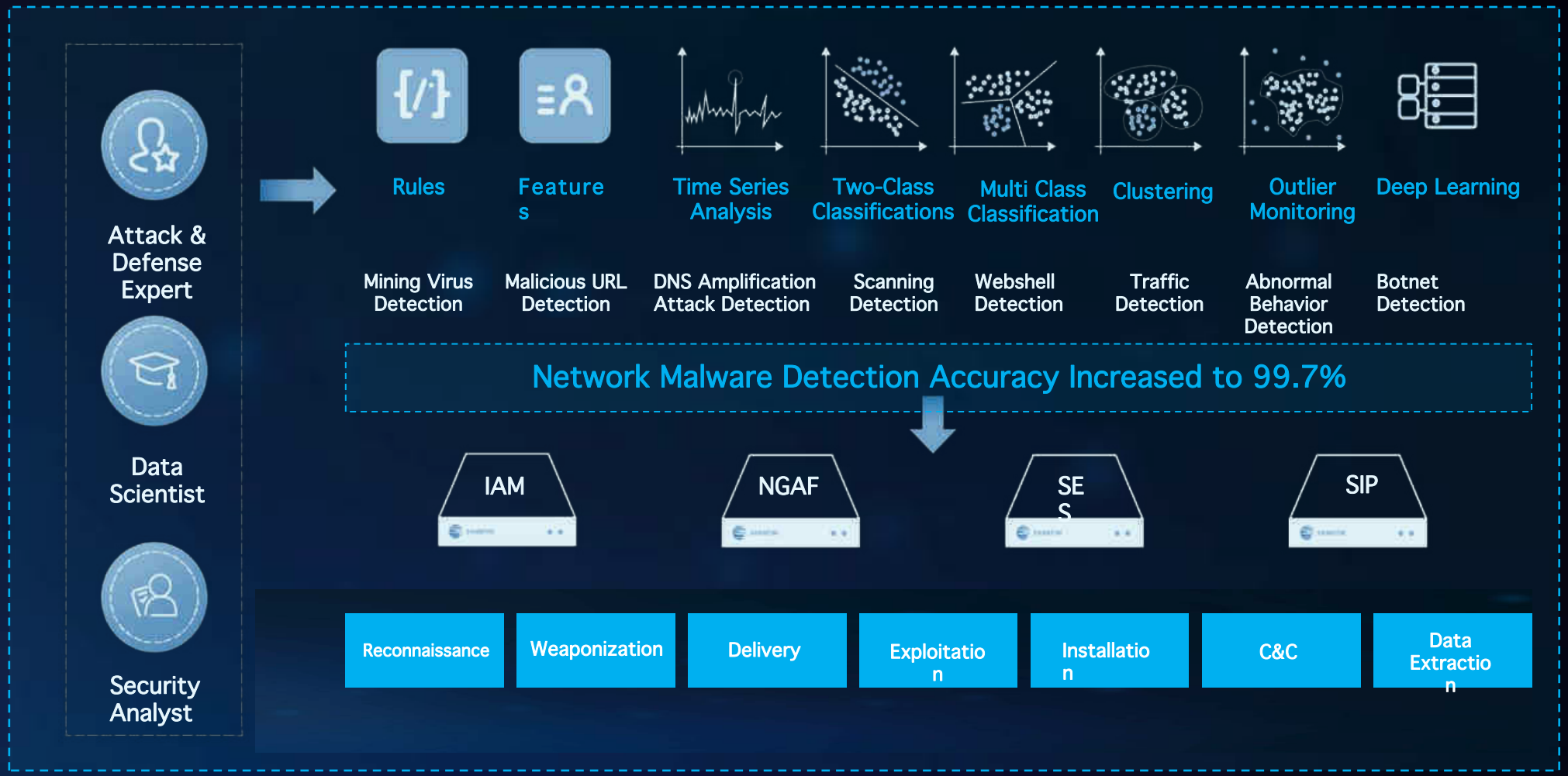


Neural-X


White Hat Researchers
Data Scientists
Security Analysts
Threat Intelligence
IP Reputation
URL Reputation
File Reputation
Security Analytics
Botnet Analysis
Sandboxing
Engine Zero
Deep Learning

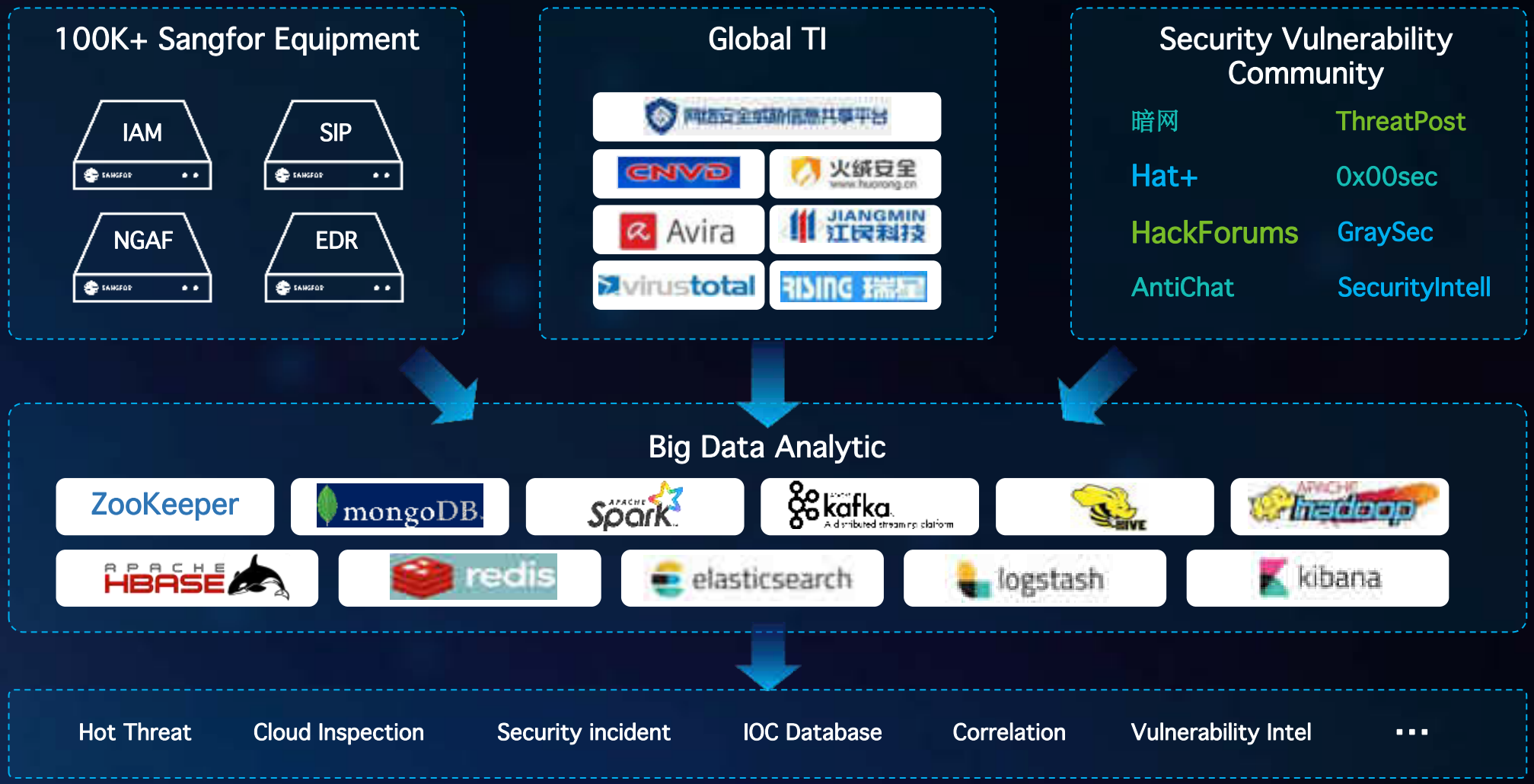
Sangfor Neural-X– Cloud Threat Intelligent

Realtime Threat Intelligent Empowers Network & Endpoint



Sangfor Neural-X– Cloud Threat Intelligent

Multidimensional Threat Intelligent



Security Capabilities from Neural-X

PART 3

Integrated Network & Endpoint

Sangfor Integrated Security Solution Architecture

Security Delivery with Integrated Network, Endpoint and Cloud Continuous Empowerment

Neural-X

- Massive Multidimensional Threat Intelligence
- Engine Zero
- Multiple Expert Rule Engine

- Real-time Cloud Detection Technology
- Big Data Intelligent Analysis & Detection
- High Real-time Collaboration between Endpoint & Cloud

Network Boundary Defense

- Server Identification
- Open Port Identification
- Sensitive Data Identification
- Vulnerability Risk Identification
- Account Risk Identification
- Configuration Risk Identification

- Vulnerability Attack Protection
- WEB Application Protection
- URL Filtering
- Engine Zero Anti-virus
- Email Security
- Webpage Anti-tampering

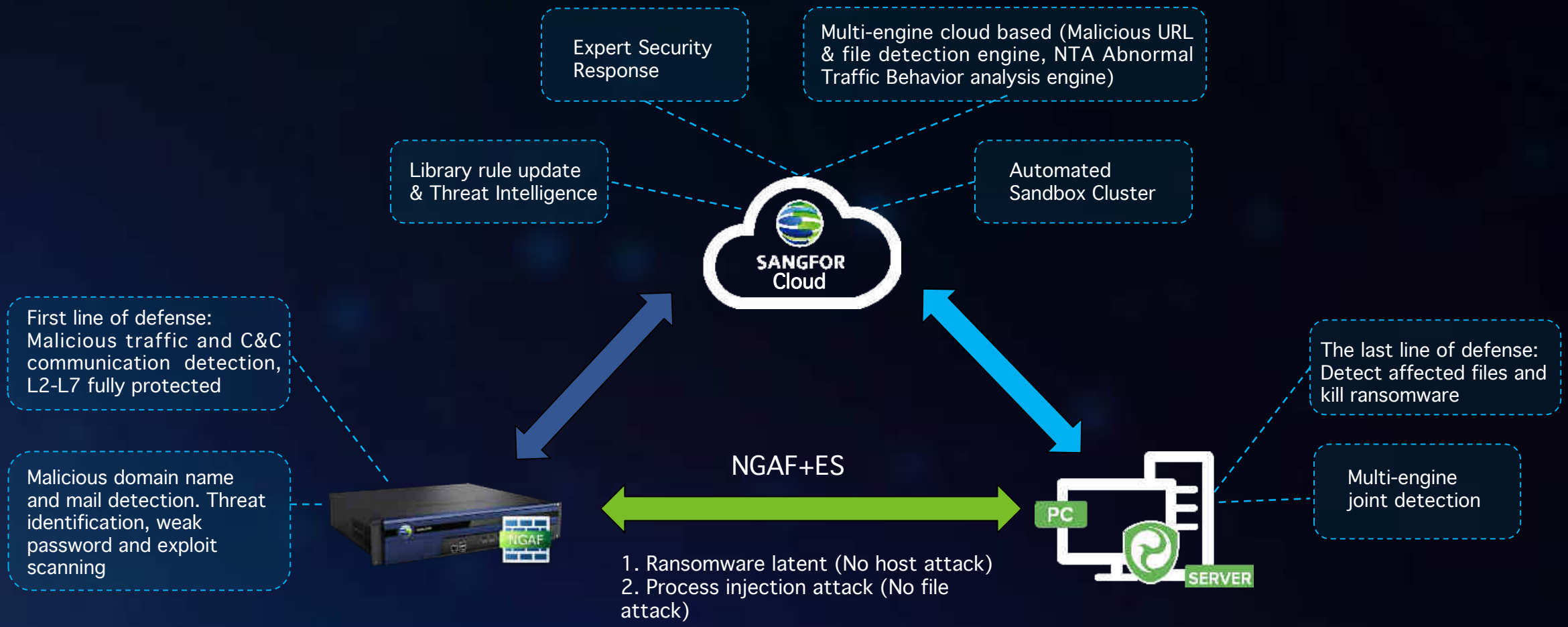
- Zombie Host Detection
- WEBSHELL Detection
- Black Chain Detection

Sangfor Endpoint Secure

Complete Risk Visibility, Comprehensive Threat Protection, Deep Inspection for Unknown Threats, Upgraded Security Operations

Helping Corporate Users to Prevent, Defend, Detect, and Respond to Threats

Sangfor's Cloud-Network-Endpoint Integrated Solution

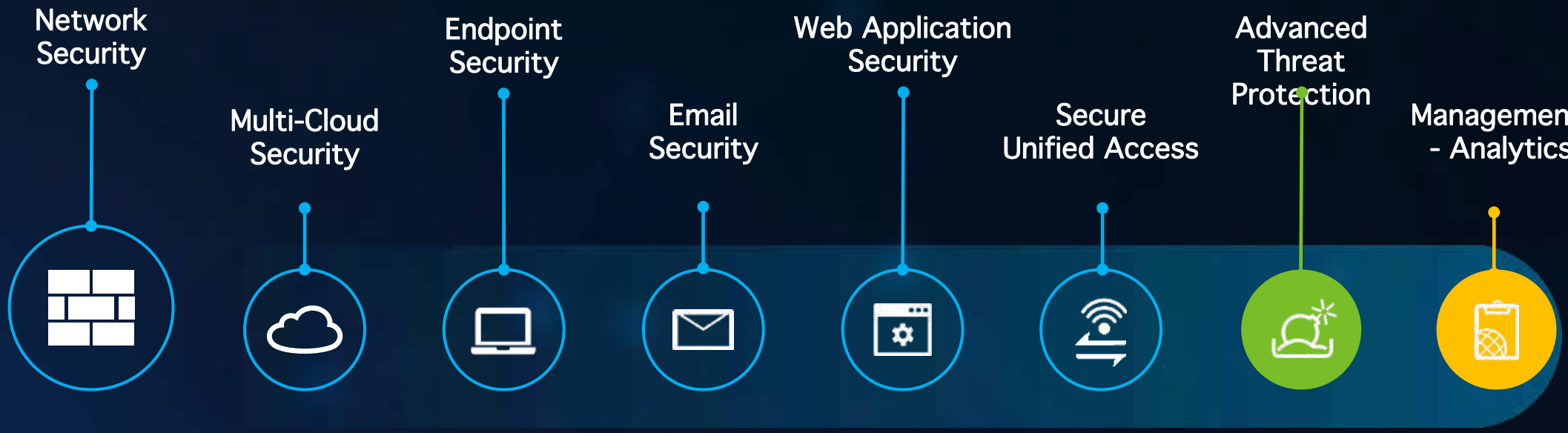


Sangfor Integrated Solution Capability

Figure 1. Value Levels of Endpoint and Network Security in Gartner

PART 4 Competitive Landscape

What's Fortinet Offering



FortiGate Enterprise Firewall

IPS

SWG

SD-WAN

FortiGate Virtual Firewall Network Security

FortiGate Cloud Firewall Network Security

FortiClient EPP

FortiMail Secure Email Gateway

FortiWeb Web Application Firewall

FortiAP Wireless Infrastructure

FortiSwitch Switching Infrastructure

FortiSandbox Advanced Threat Protection

FortiAnalyzer Central Logging /Reporting

FortiManager Central Security Management

FortiSIEM Security Information & Event Management

Fortinet Solution – Strength and Weakness

Sevice	Advanced Threat Protection (ATP)	Unified Protection (UTM)	Enterprise Protection (ENT)
Threat Intelligence Service		+  100%	
Industrial Security Service			√
Security Rating			√
CASB			√
Web Filtering		√	√
Antivirus + Sandboxing	√	√	√
IPS	√	√	√
Antispam		√	√
Internet DB	√	√	√
IP Reputation	√	√	√
Application Control	√	√	√

category	Subscription: Appliance 6: 4
PRO	• Rich models covering large-medium-and small sized enterprise • Powerful local and cloud TI capability • Opening security architecture, support be integrated by API • Provide MSSP business mode
CONS	• Real performance is only 25% of official datasheet (AC+IPS+AV) • UTM bundle price is higher by 15% • Bad reputation for protecting channel projects • Build full protection need purchase and deploy multiple security device (FortiGate + FortiAnalyzer + FortiWeb)

- Advanced Threat Protection (24x7 FortiCare plus Application Control, IPS, AV and FortiSandbox Cloud)
- Unified (UTM) Protection (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud)
- Enterprise Protection (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering, Antispam, FortiSandbox Cloud, FortiCASB, Industrial Security and Security Rating)

NGAF vs FortiGate Battle Card

SANGFOR

Features	NGAF	FortiGate
Traditional FW	Excellent	Excellent
IPS	Excellent	Excellent
Application control	Excellent	Excellent
URL Filter	Excellent	Excellent
Engine Zero (AI powered anti-malware, AV)	Excellent	Poor
E-mail Security	Poor	Excellent
Sandbox	Excellent	Excellent
Neural-X (Cloud based TI)	Excellent	Excellent
Web Application	Excellent	Average
Active Scanners	Excellent	Excellent
Security visibility, Reporting	Excellent	Poor
WiFi integration/protection	Poor	Excellent
EDR correlation	Excellent	Average
Simplified Security Operation	Excellent	Excellent
Flexible Deployment (HW, SW, VM, IaaS)	Average	Excellent
SDWAN features	Excellent	Excellent

Excellent

Average

Poor

NGAF vs FortiGate Battle Card

Features	NGAF	FortiGate
Known & Unknown Threats Protection	• Engine Zero • Neural-X	Need FortiSandbox, and additional TI subscription
Total Business System Protection	NG Application Firewall which includes: • IT assets discover • Top 10 OWASP Certified • Support web application threat signatures • HTTP Anomalies Detection • Application Hiding • AI based, and sematic engine to reduce false positive • Integrated Web Scanner & Vulnerability Scanner • Integrated Security Reporter	Need FortiWeb
Security Visibility	Integrated Security Reporter which provides holistic end-to-end security overview, from Business System to endpoint users and their correlation, detailed visibility	Overview only on Top Security status Signature Database cannot be viewed
Real Time Detection, Rapid Response	Auto-protection for pre-attack, during-attack and post-attack.	Limited Function Need to manual check on certain security logs
Simplified Operations & Management	Friendly user interface, with minimize the challenge of misconfiguration of security policies. Intuitive reporting which provides details information for management, incident response, as well as daily operations.	Operation view is not in depth for further analysis

FortiGate Gartner MQ Review

Gartner - Summary	Gartner - Cautions	Gartner - Cautions
Fortinet is a network and security player, headquartered in Sunnyvale, California. It is regularly expanding its product portfolio with FortiSIEM and FortiCASB being recent additions. The vendor's other products in the portfolio cover network security, endpoint security, SIEM, wireless access points and switches. FortiGate firewalls are still the vendor's most popular and largest selling products.	**Product Strategy:** Fortinet's product strategy is more focused on expanding its portfolio with products like FortiWeb, FortiSIEM and FortiClient, and enhancing Security Fabric features. It lacks enhancements to its firwall product. Gartner clients have reported poor presales support for smaller deals that only involve a pair of Firewall **Innovation:** Fortinet lacks in innovation in firewall features and capabilities.	**Customer Experience:** Gartner receives mixed feedback on Fortinet technical support. Gartner clients and surveyed clients have reported **poor technical support** on new product models and new features. They have also reported that the technical **support team took longer than usual** for the resolution of product- and feature-related issues.

Strength

- **Sales Execution:** Fortinet continues to be one of the most visible vendors in Gartner client shortlists for firewall by enterprise customers looking for a perimeter security use case..
- **Geographic Strategy:** Fortinet firewalls are visible across geographies and compete strongly with regional firewall vendors. The vendor has both channel and direct presence across the globe, including a large focus on developing markets.
- **Brand and reference:** FortiNe has the most certification from NSS, ICSA, CC, it has most reference globally, SMB customers can purchase small models from the market, no need any POC.

Sophos Offering

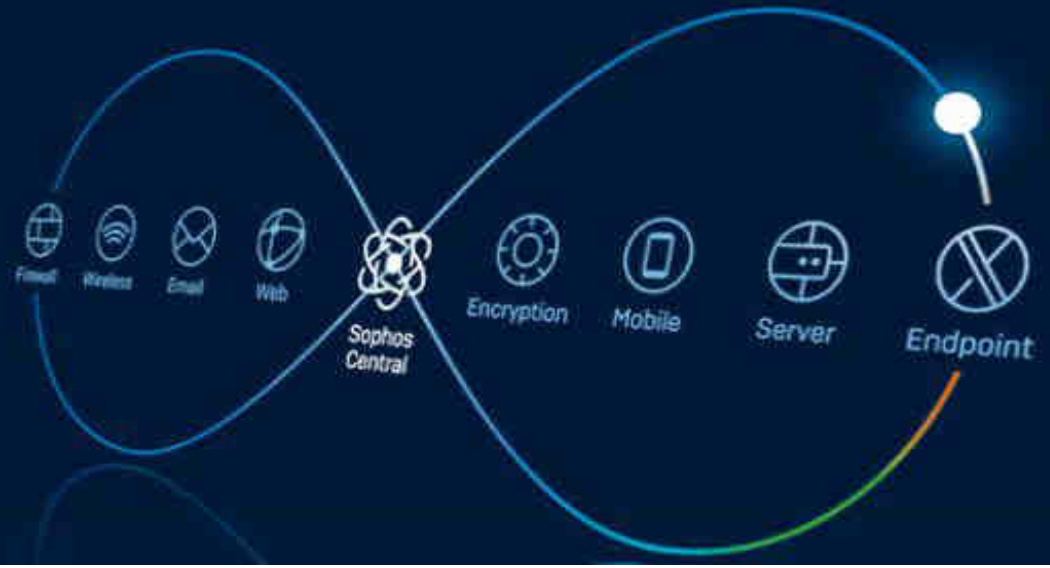
SANGFOR

CENTRAL MANAGEMENT

Synchronized Security against coordinated attacks.

Solutions that share threat intelligence and talk to each other, managed through a single, centralized interface, from firewall to endpoint.

Free Trial Learn More

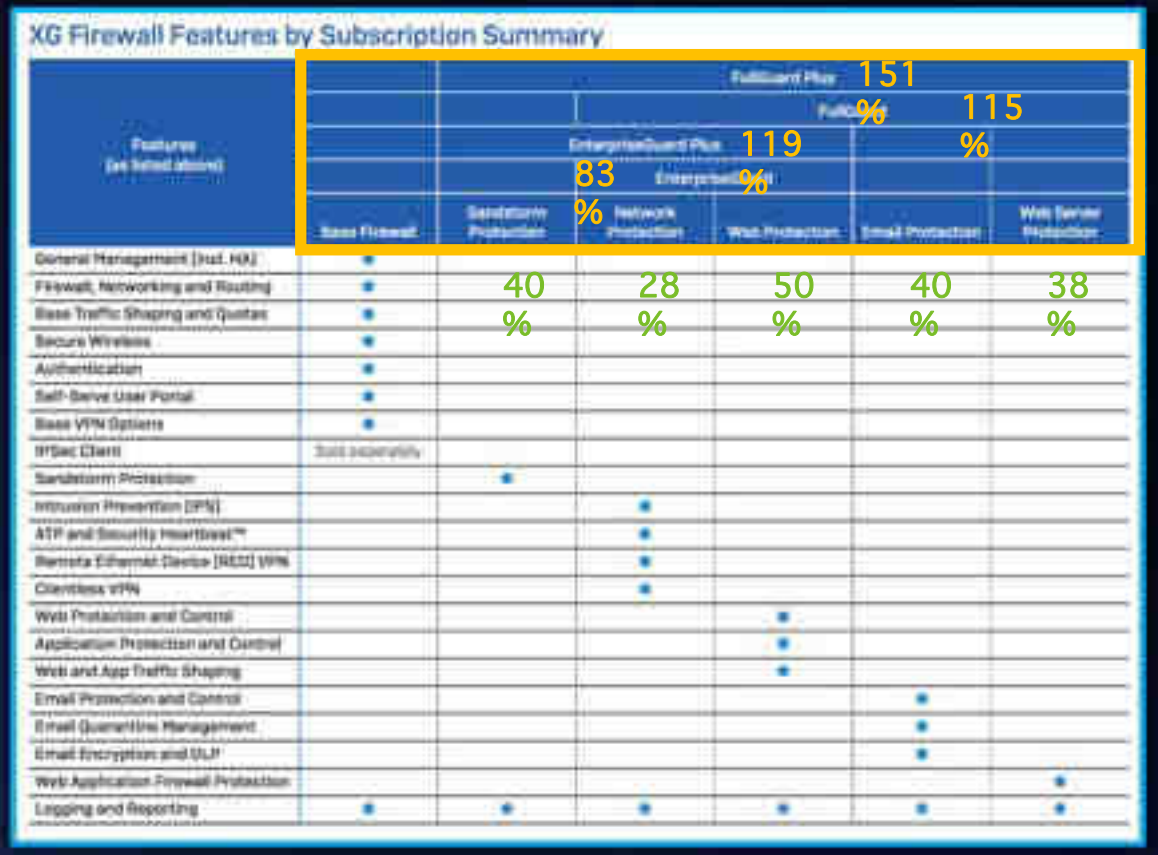


XG Firewall
Next-Gen Firewall

Intercept X
Next-Gen Endpoint

- Sophos Central
- Sophos Wireless
- Sophos Email
- Sophos Mobile
- Phish Threat
- UTM
- Intercept X for Server
- SafeGuard Encryption
- Secure Web Gateway

Sophos Solution – Strength and Weakness



XG Series Appliance

Category	Subscription: Appliance 8: 2
PRO	• Powerful endpoint protection solution • Cloud TI+XGxx+EDR synchronized solution is very competitiveness • Unified platform for visibility and security event operation • Competitive price in SMB market
CONS	• Real performance is only 15% of official datasheet（AC+IPS) • Complex and bad effect of WAF model • Defend against unknown threats need to use sandstorm function with 40% cost of hardware price

NGAF vs Sophos Battle Card

Features	NGAF	SOPHOS
Traditional FW	●	●
IPS	●	●
Application control	●	●
URL Filter	●	●
Engine Zero (AI powered anti-malware, AV)	●	●
E-mail Security	● (No anti-spam)	●
Sandbox	●	●
Neural-X (Cloud based TI)	●	●
Web Application	●	●
Active Scanners	●	
Security visibility, Reporting	●	● Requires iView Subscription
WiFi integration/protection	●	●
EDR, File encryption, correlation	●	●
Simplified Security Operation	●	●
Flexible Deployment (HW, SW, VM, IaaS)	●	●

● Excellent

● Average

● Poor

NGAF vs Sophos Battle Card

Features	NGAF	SOPHOS
Total Business System Protection	Support Application Firewall which includes: • IT assets discover • Top 10 OWASP Certified • Support web application threat signatures • HTTP Anomalies Detection • Application Hiding • AI based, and sematic engine to reduce false positive • Integrated Web Scanner & Vulnerability Scanner • Integrated Security Reporter	Basic WAF Features Requires 3rd Party Vulnerability Scanner Internal reporting tools required integration with Vulnerability Scanner
Security Visibility	Integrated Security Reporter which provides holistic end-to-end security overview, from Business System to endpoint users and their correlation, detailed visibility	Overview only on Top Security status Signature Database cannot be viewed
Real Time Detection, Rapid Response	Auto-protection for pre-attack, during-attack and post-attack.	Limited Function Need to manual check on certain security logs
Simplified Operations & Management	Friendly user interface, with minimize the challenge of misconfiguration of security policies. Intuitive reporting which provides details information for management, incident response, as well as daily operations.	Operation view is not in depth for further analysis

Real World Security Effectiveness Comparison

IPS

Equipment	Policy	Vulnerability Attack	Vulnerability Blocked	Block Rate
NGAF	Default	34	29	85%
Fortigate	Default	34	26	67%
Sophos	Default	34	16	47%

WAF

Equipment	Policy	Vulnerability Attack	Vulnerability Blocked	Block Rate
NGAF	Default	379	379	100%
Fortigate	Default	379	234	61%
Sophos	Default	379	56	14%

Known Malware

	Policy	Malware Sample	Malware Blocked	Block Rate
NGAF	Default	300	299	99.67%
Fortigate	Default	300	180	60.00%
Sophos	Default	300	50	16.67%

Unknown Malware

	Policy	Malware Sample	Malware Blocked	Block Rate
NGAF	Default	43	43	100.00%
Fortigate	Default	43	2	4.65%
Sophos	Default	43	43	100.00%

PART 6

Sangfor NGAF Proven Reputation

No.1 Branding, Enterprise Grade

July11
China First
NextGen Firewall

Jan13
OWASP 4 stars
Certified
Top in China

July14
2nd NextGen Firewall
Set the Standard

Aug14
NSS Labs
Top
Rated

Dec14
Selected by
Enterprise

May15
ICSA Certified
Only 4 Players
in China

15.06
Reported in the
first time
Gartner

Aug15
First in China
2nd Gen Firewall

June16
Gartner Technology
Trend
No.1 in China

5 Years Continuously Listed On Magic Quadrant

Notable NGAF Customer

SANGFOR

THANK YOU

www.sangfor.com

Sangfor Technologies Inc.