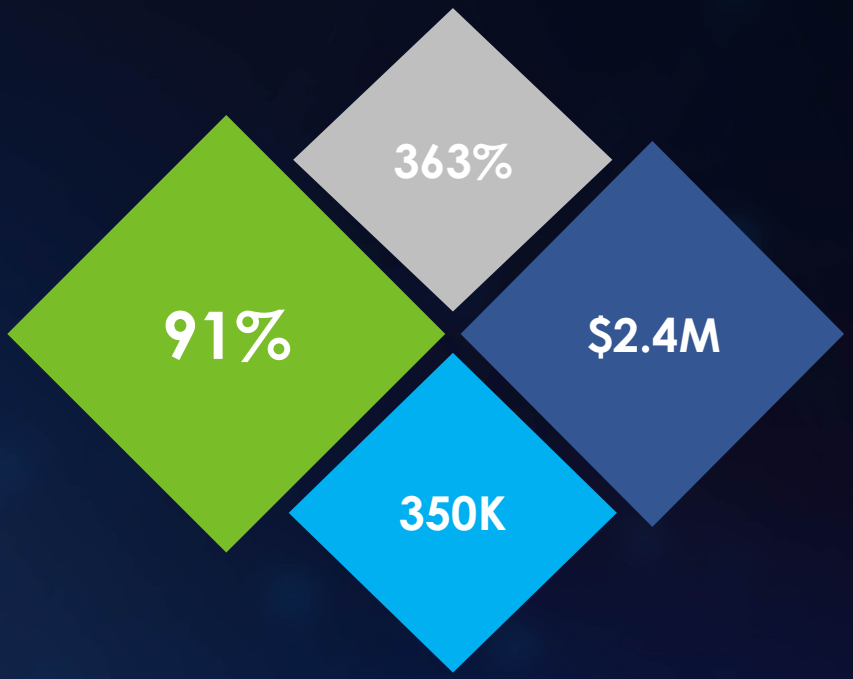
SANGFOR

Endpoint Secure

The Future of Endpoint Security

PART 1 The Threat

The Threat



01 **Cyber attacks that begin with phishing**

- TrendMicro

02 **Increase of Ransomware attacks annually**

- Malwarebytes

03 **New malicious malware samples seen everyday**

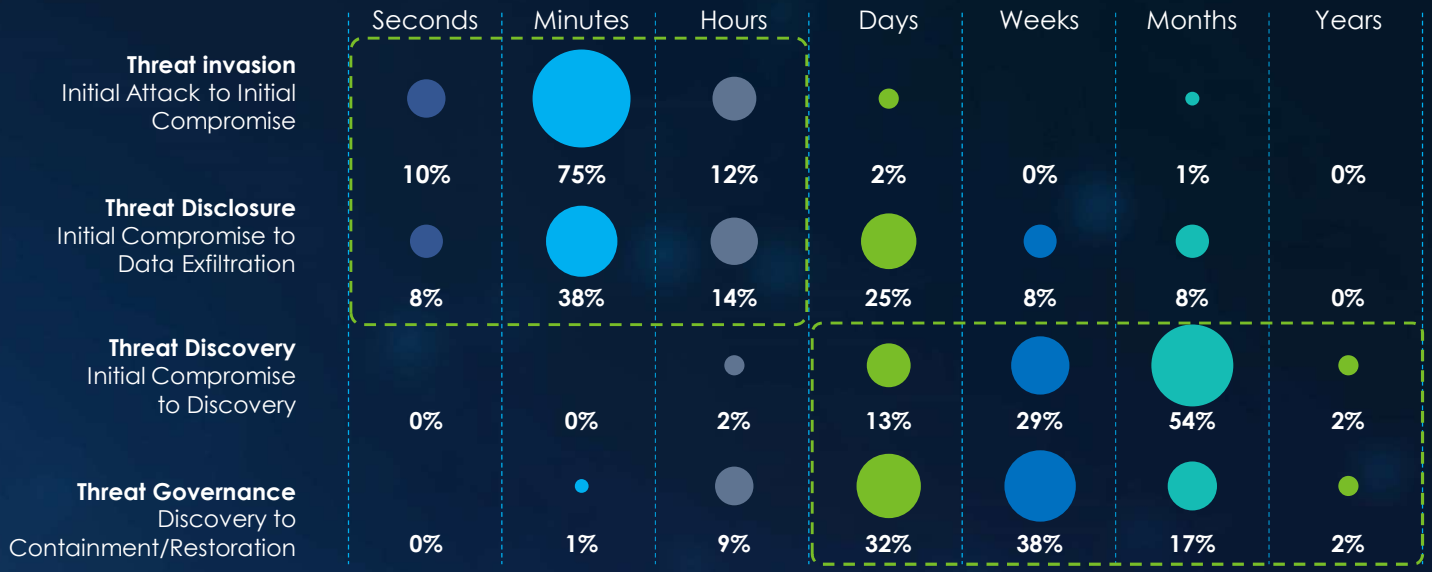
- AV Test

04 **Average cost of a malware attack to a company**

The longer discovery of a breach takes, the more it costs.

- Accenture

Response Is Inadequate



- 85% of invasions are completed within minutes.
- 229 days is average time to discovery in APAC

Normal patching process takes too long allowing uncontrolled rapid malware spread

The business impact increases the longer malware is undiscovered

The Fall of Traditional and Next Generation Antivirus

SANGFOR

Limited Protection Against Coming Unknown & Advanced Persistent Threats

Overconfidence

Assumes Will Detect & Block Everything

- Testing shows only 99.5% effective

Inadequate Defence

Behaviour Analysis

- Identifying behavior inadequate against new modular malware

Outdated Defence

Signature DB

- Signatures ineffective against new modular malware

Emphasis on Detection

Response is Inadequate

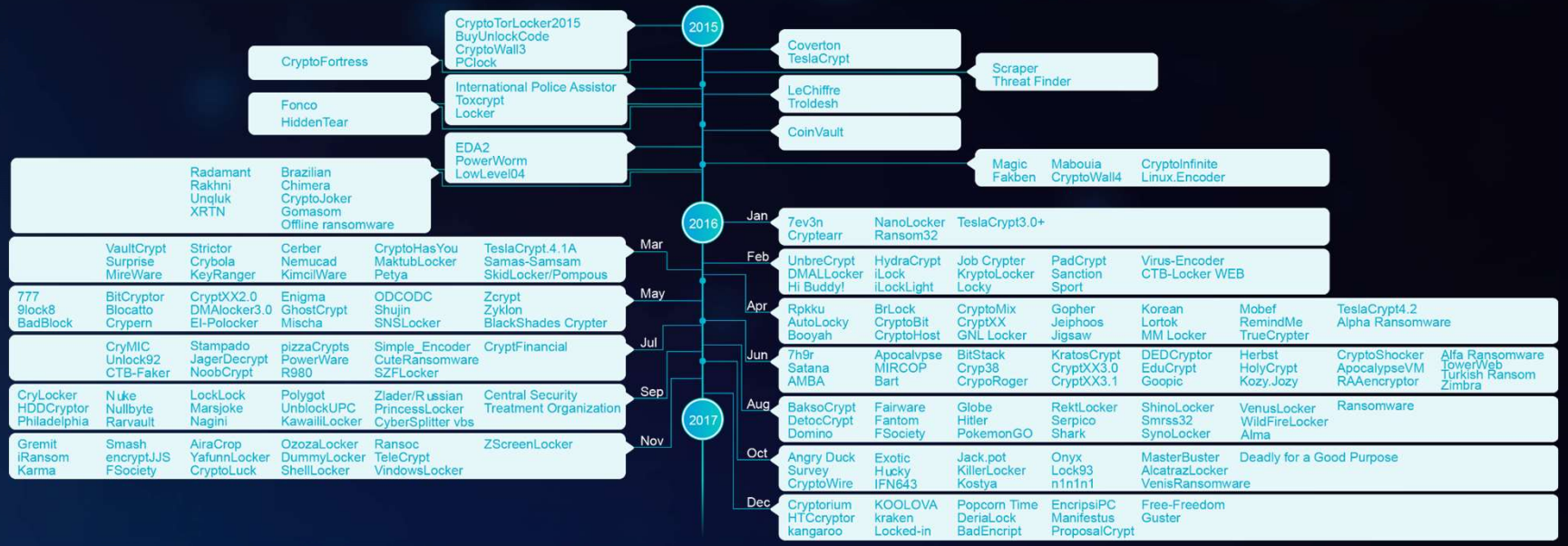
- Limited ability to contain and mitigate a breach

Ransomware Bypasses Traditional & Next Gen Antivirus

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



PART 2

Endpoint Secure

The Future of Endpoint Security

Sangfor Security Architecture

Fully Protected Network, Endpoint & Cloud

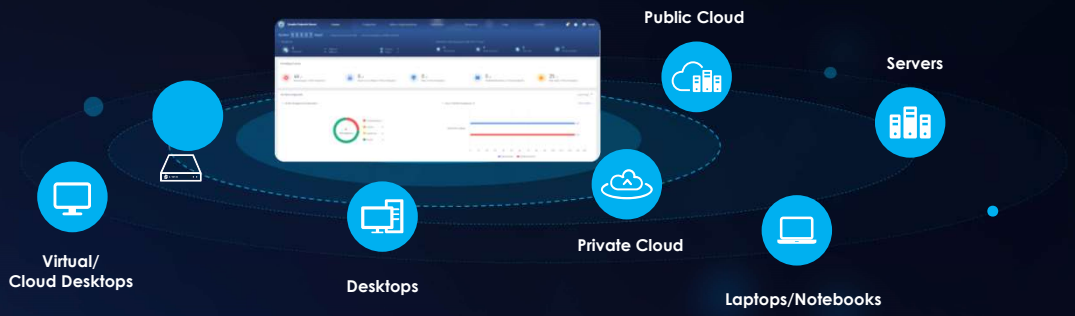
Correlation, Detection & Response

Continuous Evolution of Capabilities Using Cloud-Based TI & AI

Security Operations Managed Service

Endpoint Secure

The Future of Endpoint Security



Enterprise Asset Integration Strategy

Operating Systems

Windows, Centos, Ubuntu, redhat, Suse, Debian, Red flag Linux, Red Flag Asianux, Winning Kirin, Oracle Linux

Virtualization

VMware, Huawei, Nutanix, Sangfor HCI, Hua San H3 Cloud, SmartX, Zstack, Alibaba, Tencent

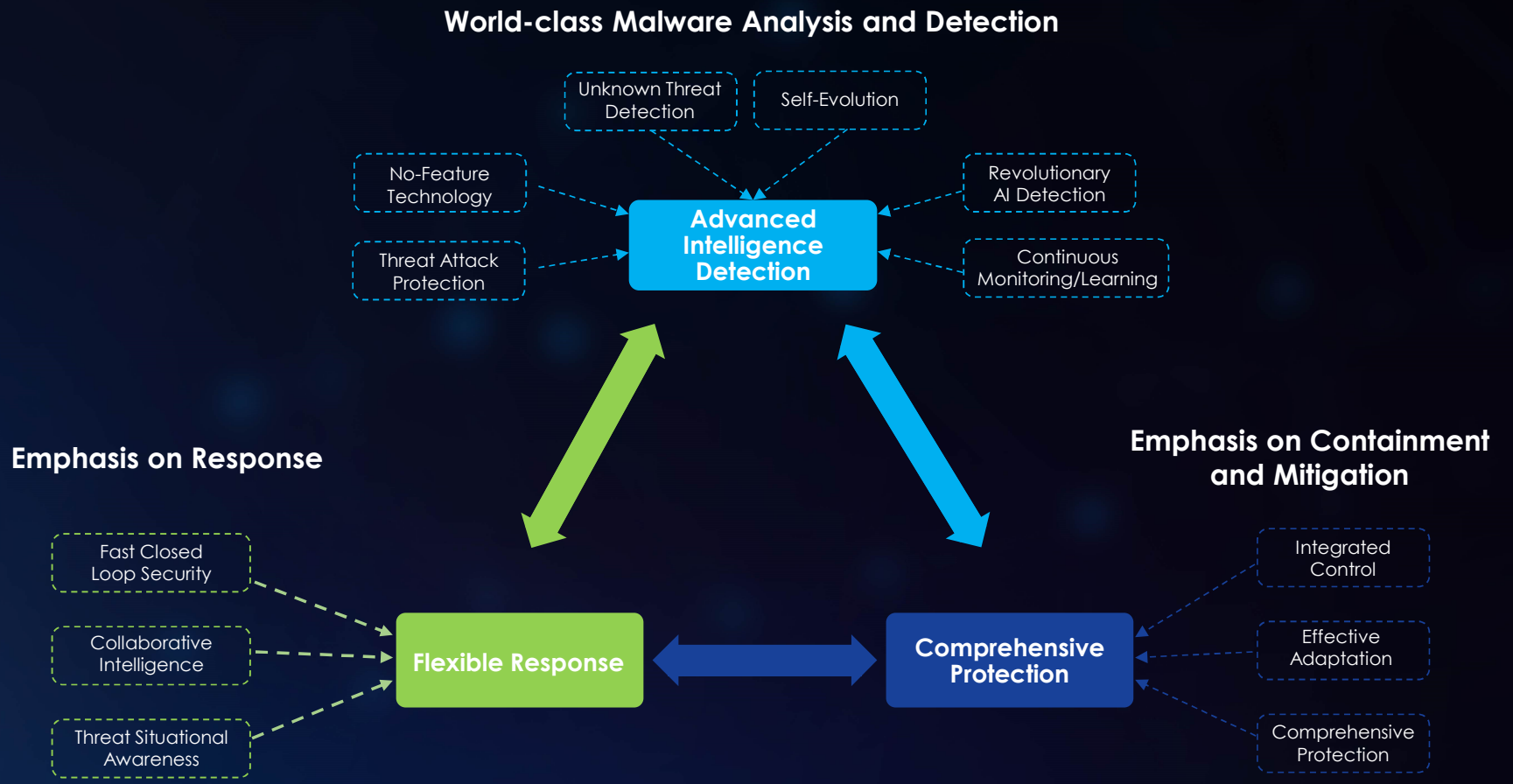
A Different Approach For Defending Endpoints

AI powered protection using Neural-X and Engine Zero

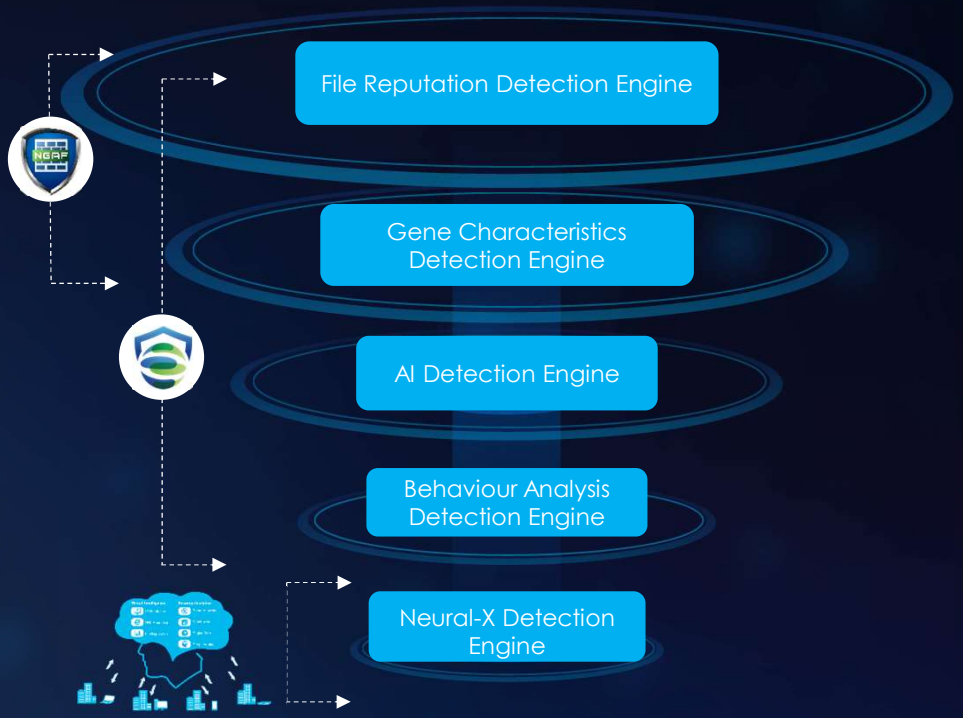
On-premise, Cloud-based or Hybrid Management for Scalability

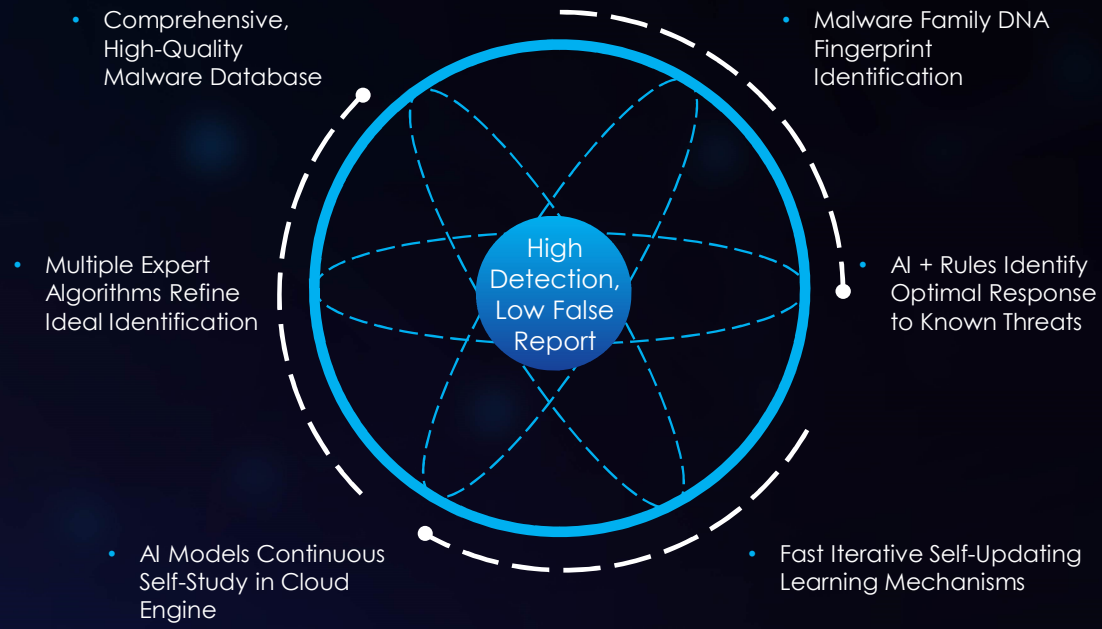
Direct Integration with Sangfor NGAF

A Different Approach for Defending Endpoints



Predictive Attack Capability with Engine Zero





Smarter Detection Powered by AI

Sangfor Engine Zero

AI Malware Detection Engine

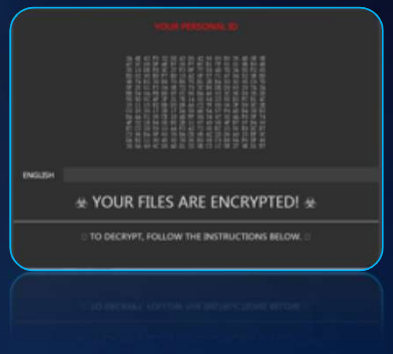
Innovative Unique AI Technology

High Detection Accuracy

Low False Positive Rate

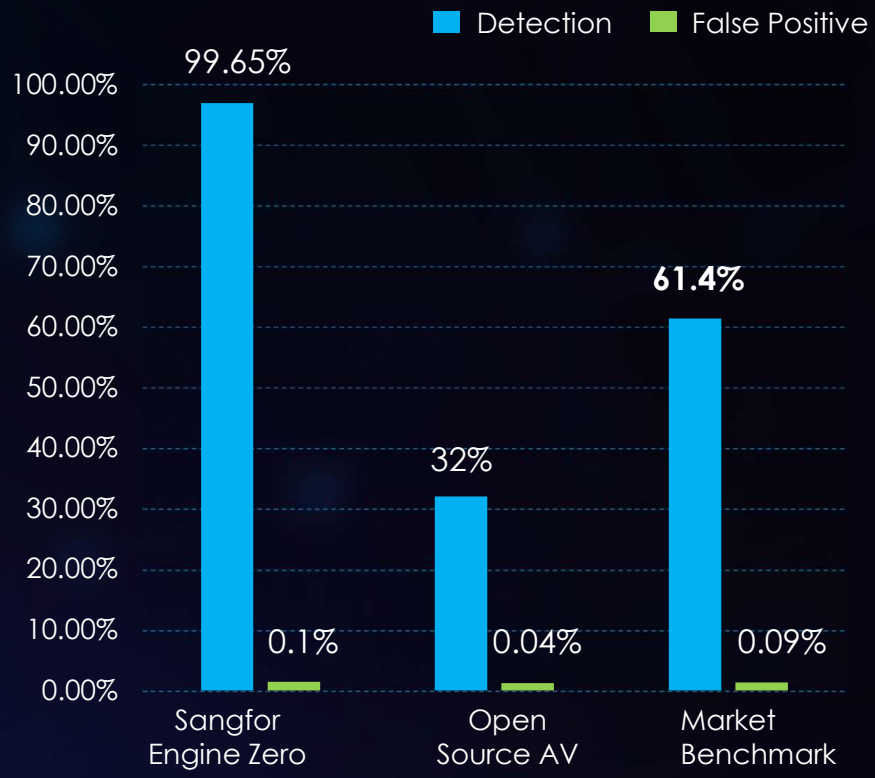
99.65% Accuracy with Unknown Malware Detection

>99.9% Accuracy with Known Malware Detection

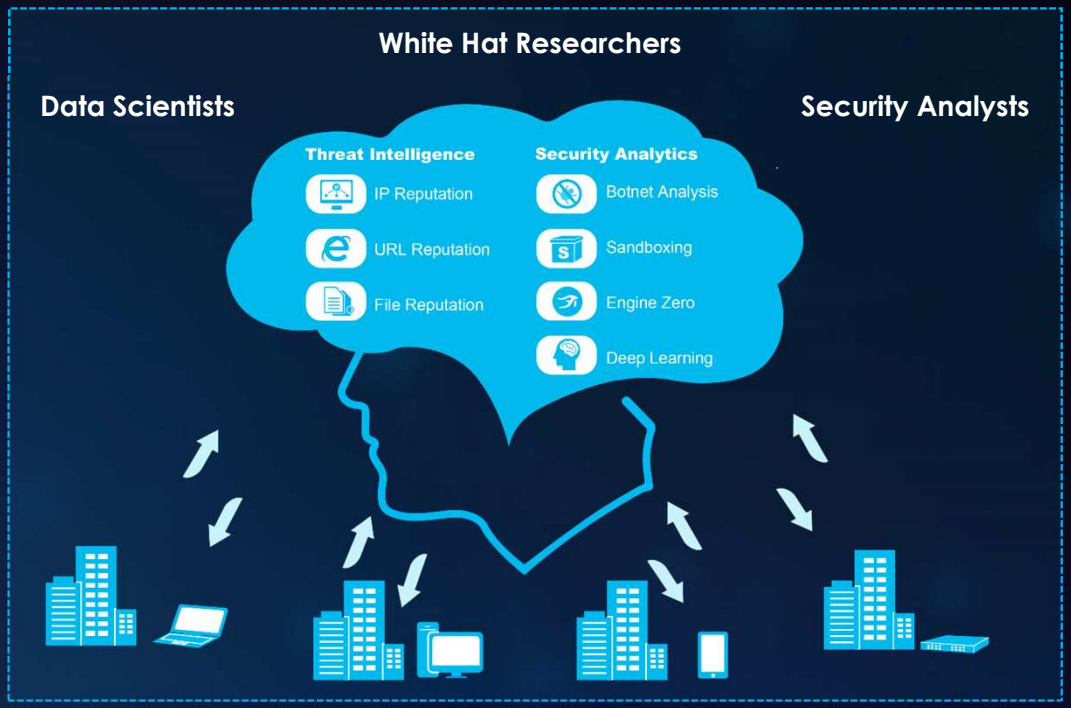


GlobeImposter Ransomware

Zero-Day Detection



Neural-X: AI Enabled Cloud Platform for Threat Intelligence & Analytics



- Real-Time Unknown Threat Detection
- Cloud Sandbox
- Fast Response

- 30K Devices Share Intelligence
- 33 Billion Requests/day
- 60+ Countries

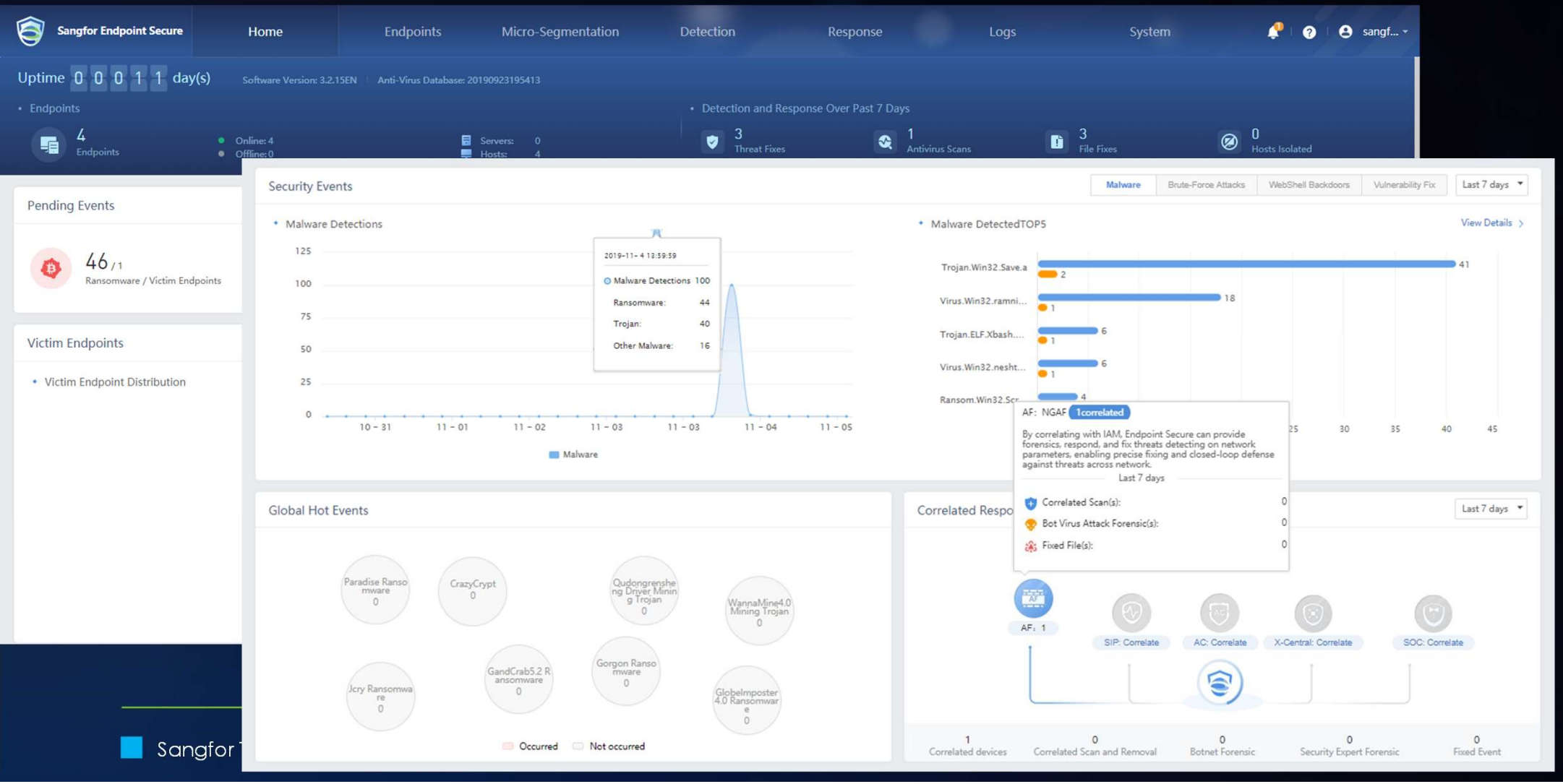
Simpler Smarter Monitoring

SANGFOR

Multi-Dimensional Response

Security Visibility

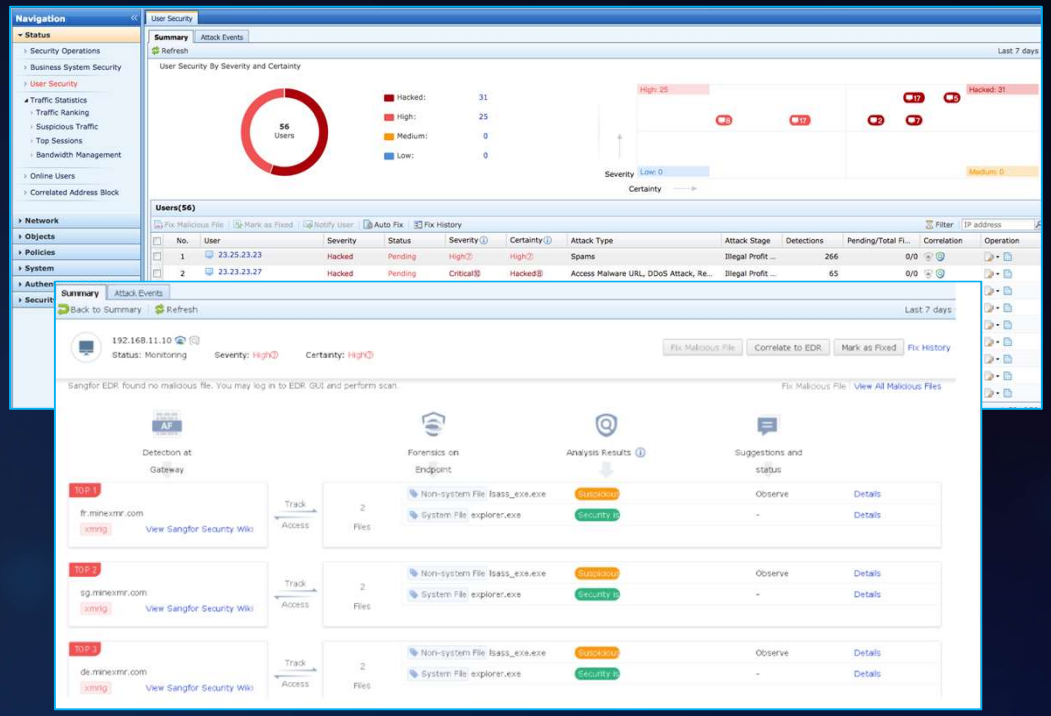
SANGFOR



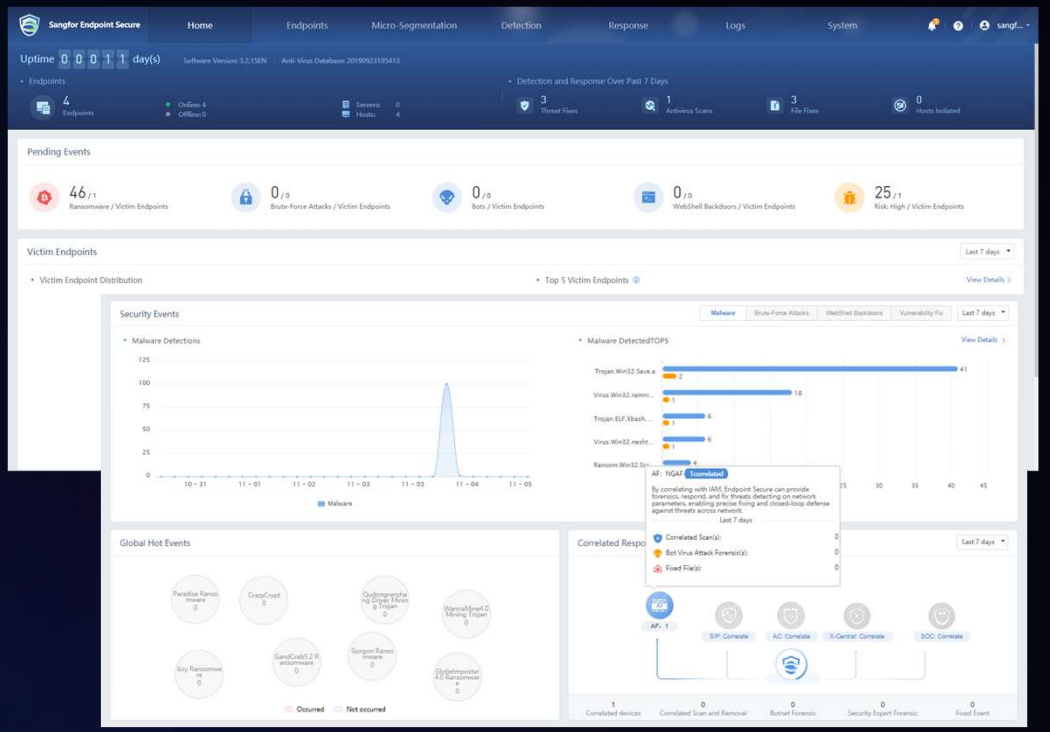
Detection

Risks to both PCs and servers are visible

NGAF Network View



Endpoint Secure Client View



Endpoint Secure Total Visibility of Enterprise Assets

Visibility of Assets

Identify core business system assets

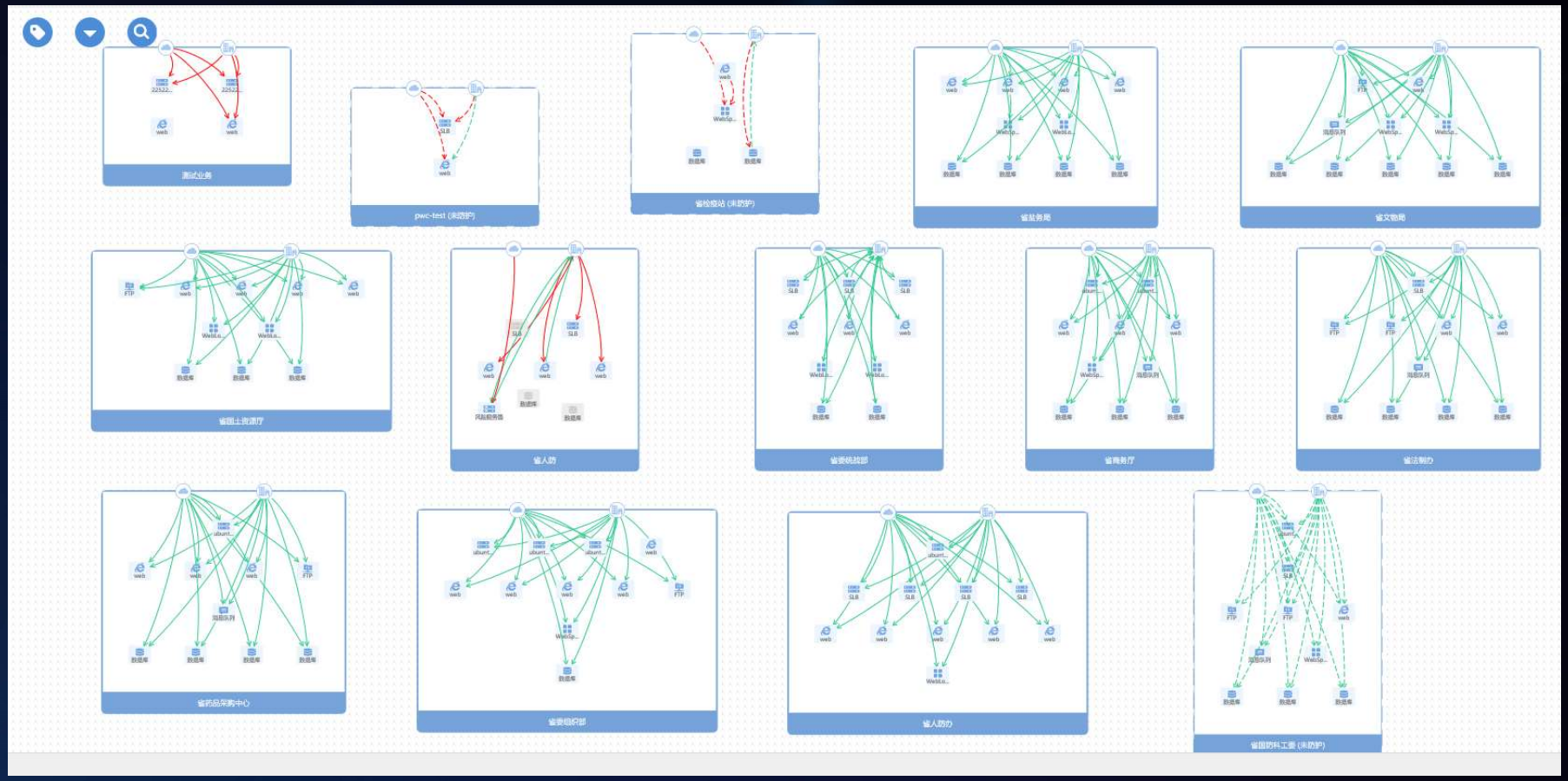
Visibility of Threats and Risks

Identify vulnerabilities and risks to business assets

Visiblity of Asset Behavior

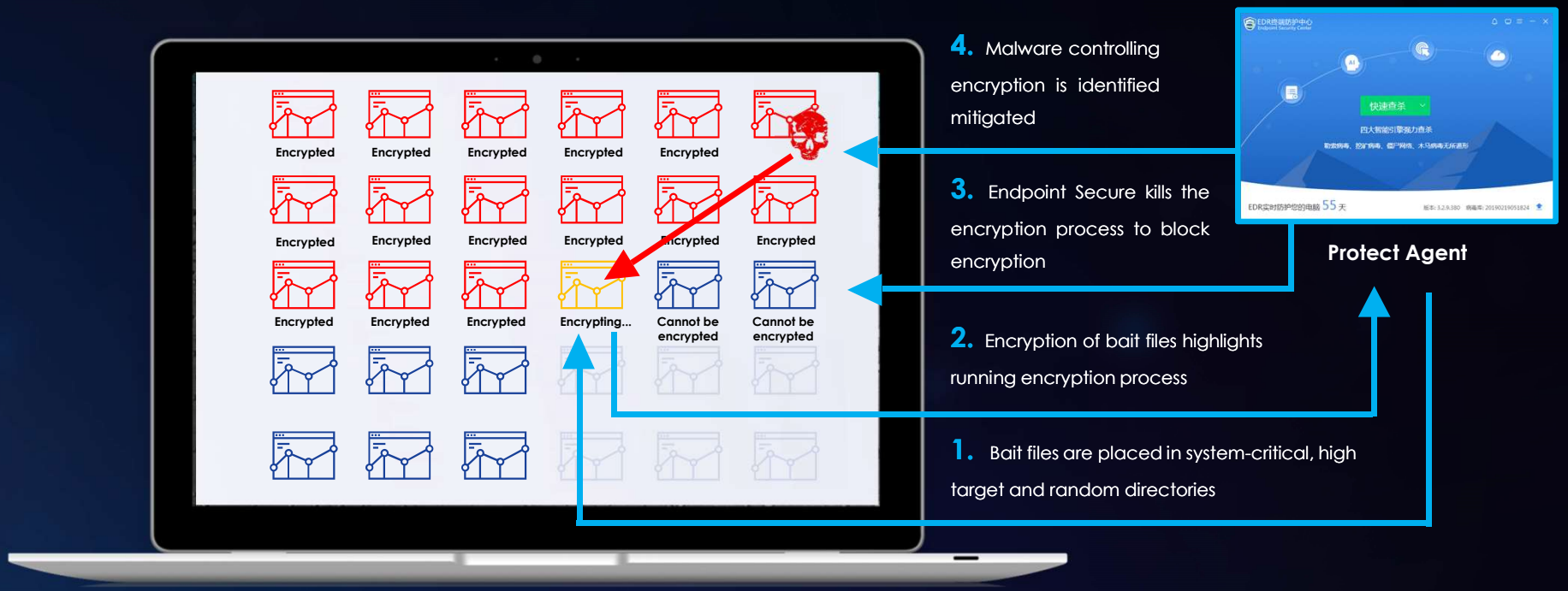
Distinguish between common and uncommon asset behavior

Identify Communications Between Endpoints



Ransomware Honeypot

After analysis of tens of thousands of ransomware, key directories with a high probability of being targeted for encryption have been identified

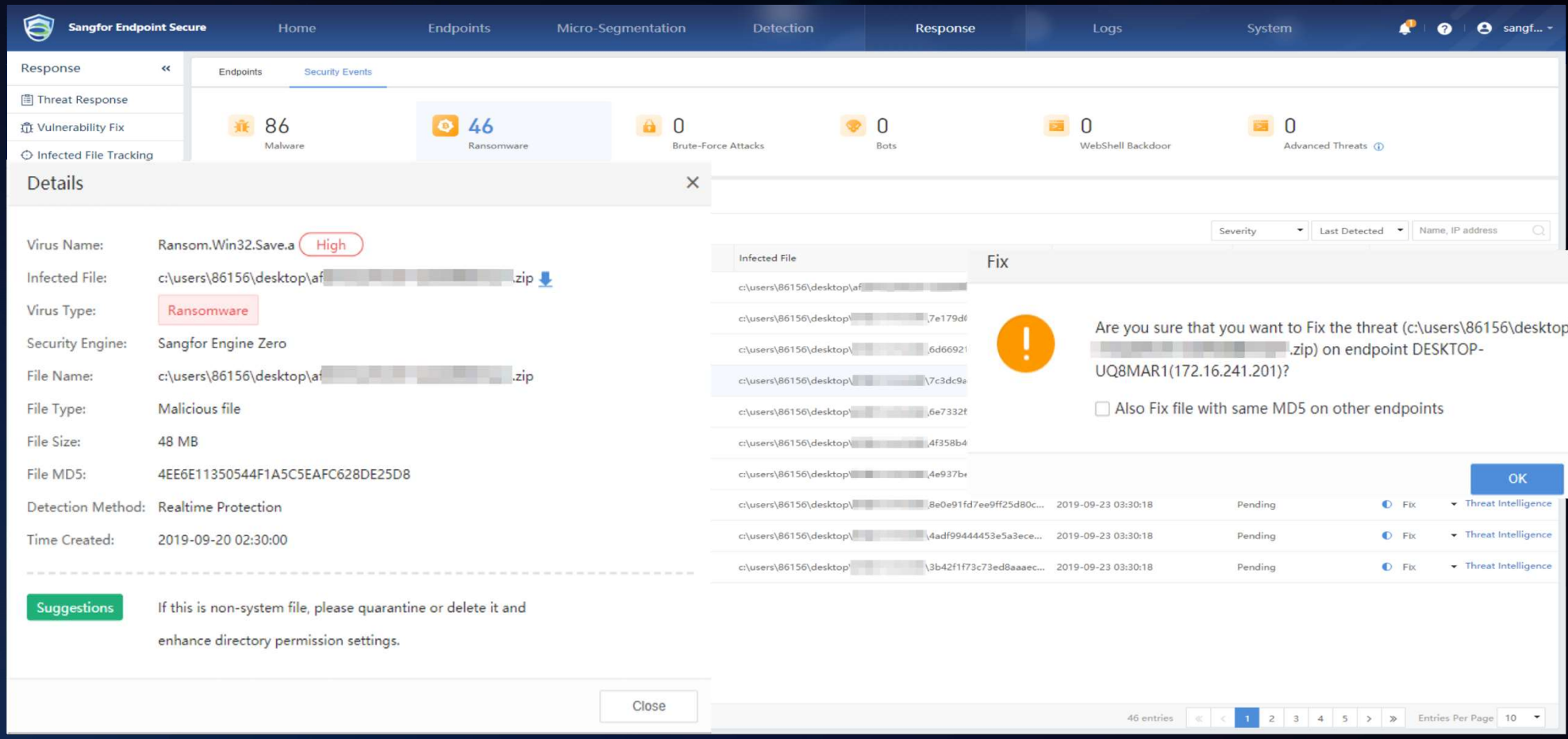


Simpler Smarter Response

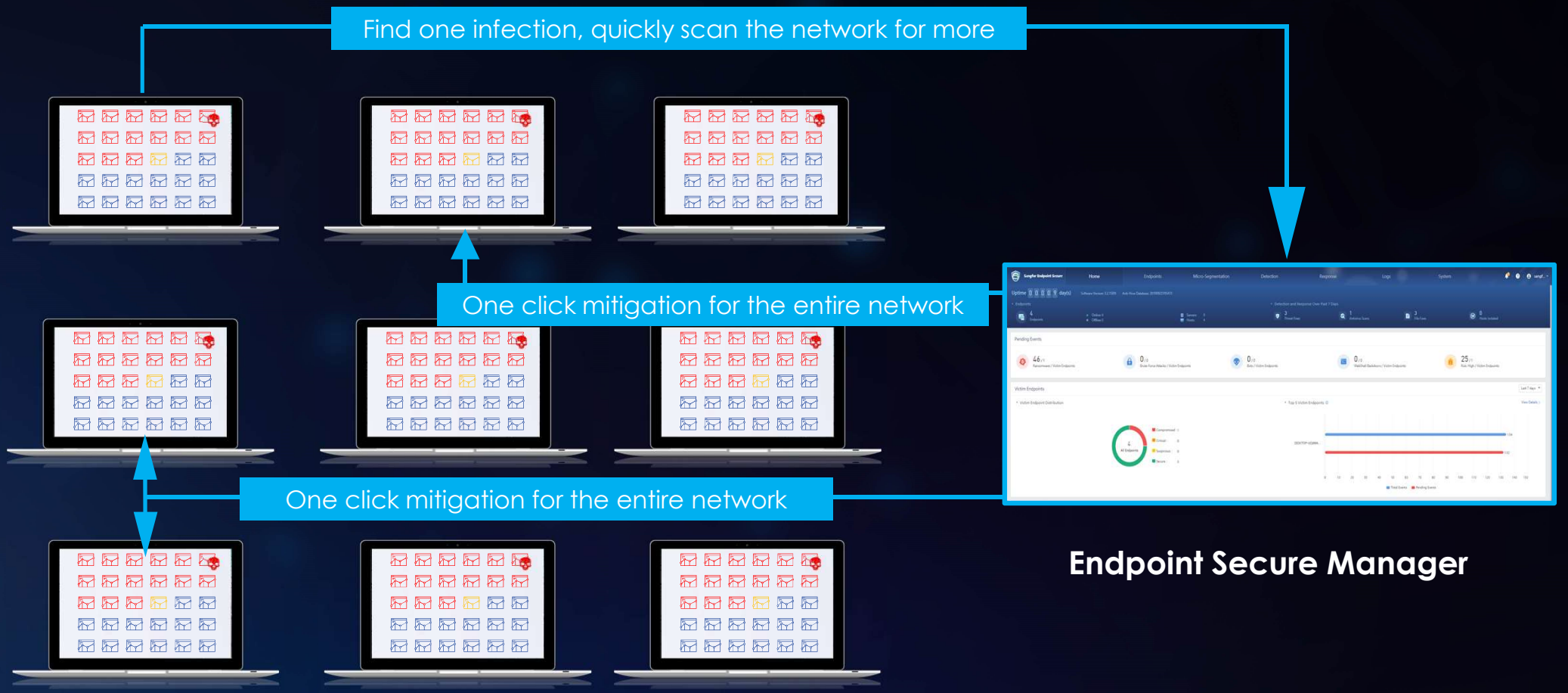
SANGFOR

Multi-Dimensional Response

Response

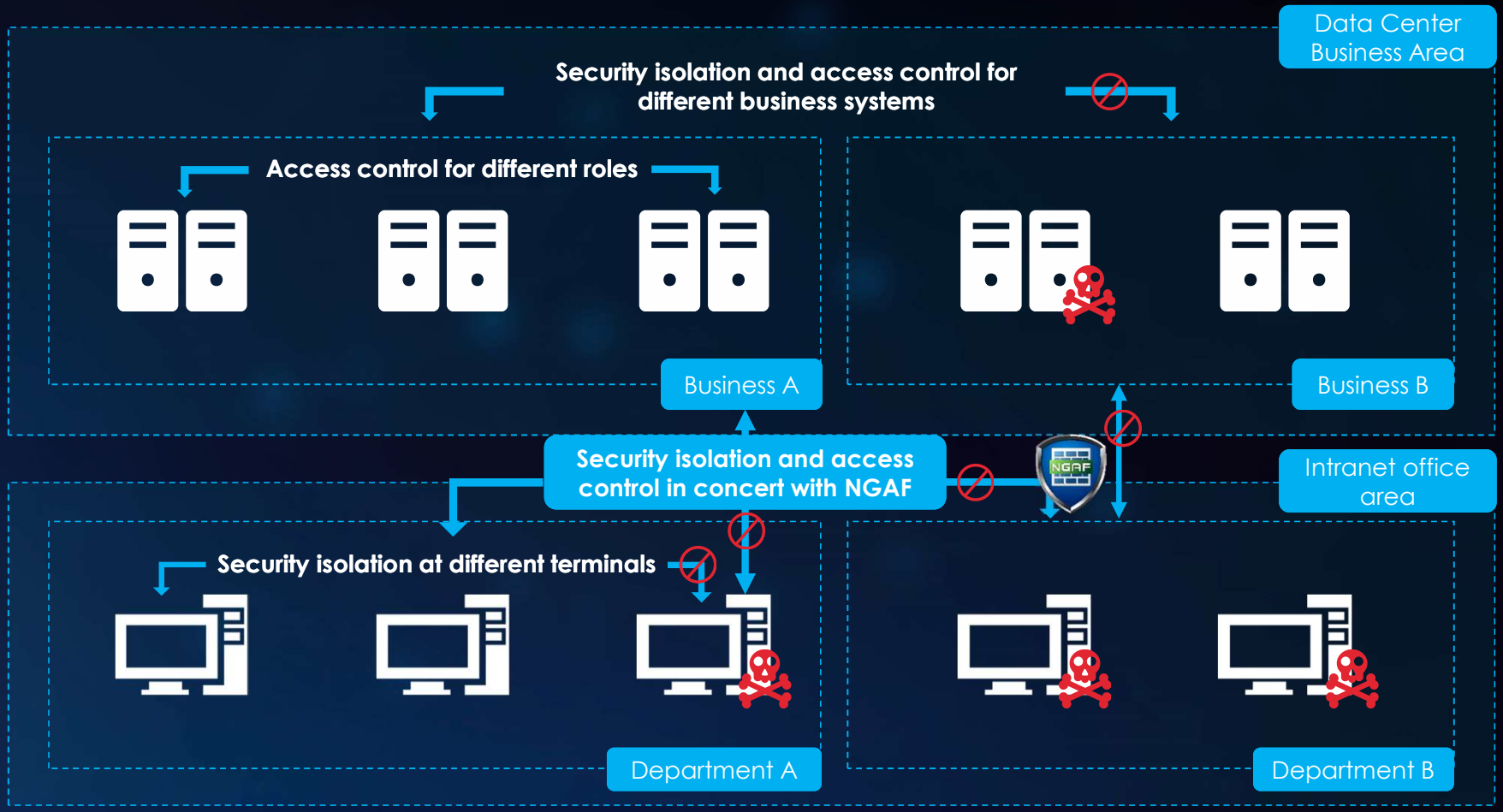

Sangfor Endpoint Secure
Home
Endpoints
Micro-Segmentation
Detection
Response
Logs
System
Response
Threat Response
Vulnerability Fix
Infected File Tracking
Endpoints
Security Events
86
Malware
46
Ransomware
0
Brute-Force Attacks
0
Bots
0
WebShell Backdoor
0
Advanced Threats
Details
Virus Name: Ransom.Win32.Save.a High
Infected File: c:\users\86156\desktop\af .zip
Virus Type: Ransomware
Security Engine: Sangfor Engine Zero
File Name: c:\users\86156\desktop\af .zip
File Type: Malicious file
File Size: 48 MB
File MD5: 4EE6E11350544F1A5C5EAFC628DE25D8
Detection Method: Realtime Protection
Time Created: 2019-09-20 02:30:00
Suggestions
If this is non-system file, please quarantine or delete it and enhance directory permission settings.
Close
Severity
Last Detected
Name, IP address
Infected File
Fix
Are you sure that you want to Fix the threat (c:\users\86156\desktop\af .zip) on endpoint DESKTOP-UQ8MAR1(172.16.241.201)?
Also Fix file with same MD5 on other endpoints
OK
Cancel
2019-09-23 03:30:18
Pending
Fix
Threat Intelligence
46 entries
Entries Per Page 10

One-Click Kill



Endpoint Secure Manager

Micro-isolation reduces threat propagation



Risk Protection for Ransomware

SANGFOR

Neural-X

- Global/Local
- Threat Intelligence
- AI Engine
- Automated Sandbox Cluster

SANGFOR

Cloud

Platform-X

- Integrated Management
- Situational Threat Awareness

MSS

Incident Response Services

NGAF

- Email
- Ransomware Detection
- Malicious Domain
- C&C Servers

Endpoint Secure

- Connection Analysis
- Malware Containment

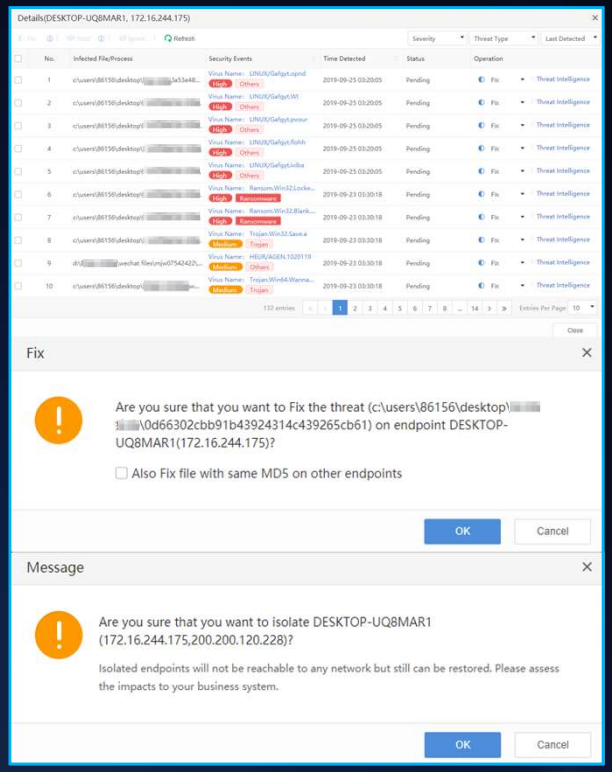
Ransomware/APT

- Detection
- Blocking
- Disinfection

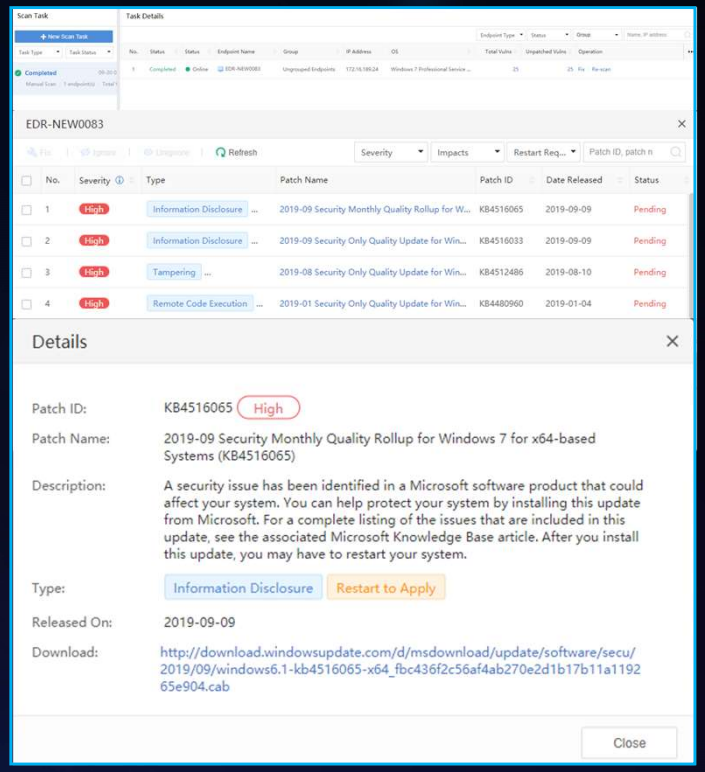
Ransomware → Infected? → C&C Communication → Lateral Propagation → Encryption

- **Risk Driven**
- **Full Protection**
- **Active Defense**

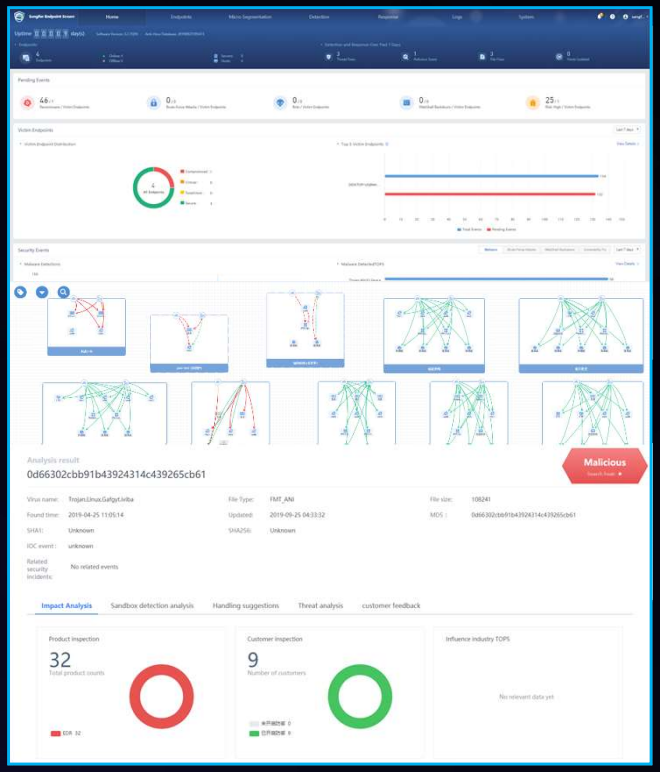
Simplified Security Operation



One Click Mitigation



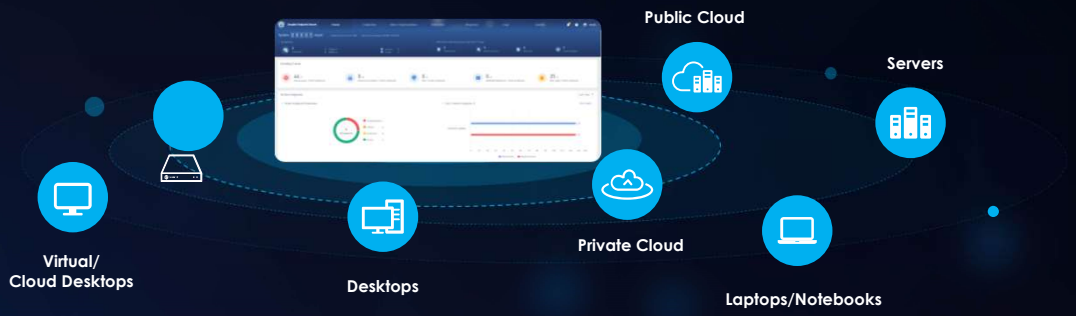
Vulnerability Scan with Remediation



Informative Visual Dashboard & TI

Endpoint Secure Requirements

The Future of Endpoint Security



Enterprise Asset Integration Strategy

Operating Systems

Windows, Centos, Ubuntu, redhat, Suse, Debian, Red flag Linux, Red Flag Asianux, Winning Kirin, Oracle Linux

Virtualization

VMware, Huawei, Nutanix, Sangfor HCI, Hua San H3 Cloud, SmartX, Zstack, Alibaba, Tencent

Linux host or VM

- 64-bit Ubuntu or CentOS
- CPU: 4 cores
- Memory: min 8GB RAM
- Disk: min 500GB

HCI and VMWare support

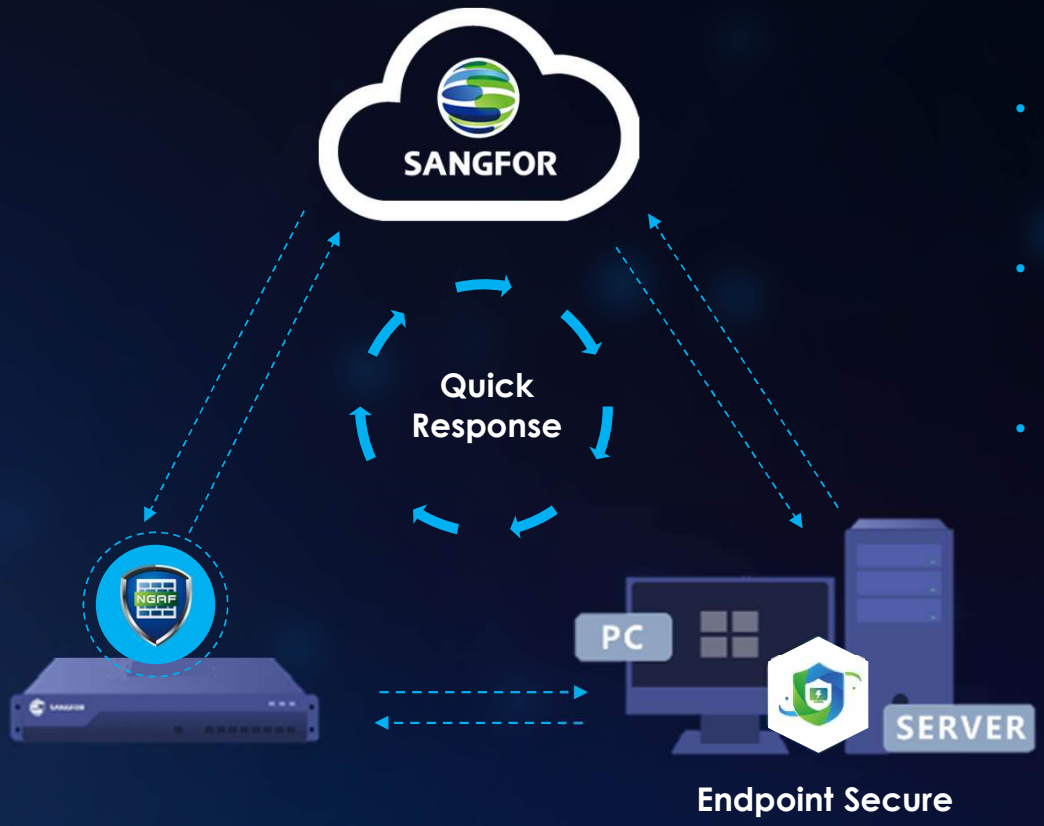
Ports Required

- 443 for downloading agent
- 8083 for services
- 54120 for management

Agent

- Less than 200MB memory
- Less than 150 MB disk
- Co-exists with other NGAV

Simpler, More Secure and Valuable with Endpoint Secure



- Simplifies Security Operation and Maintenance
- Comprehensive Solution Still Integrates with Others
- Governance, Holistic Reports and evidence

TCO

SANGFOR

THANK YOU

www.sangfor.com

Sangfor Technologies Inc.