



Endpoint Secure

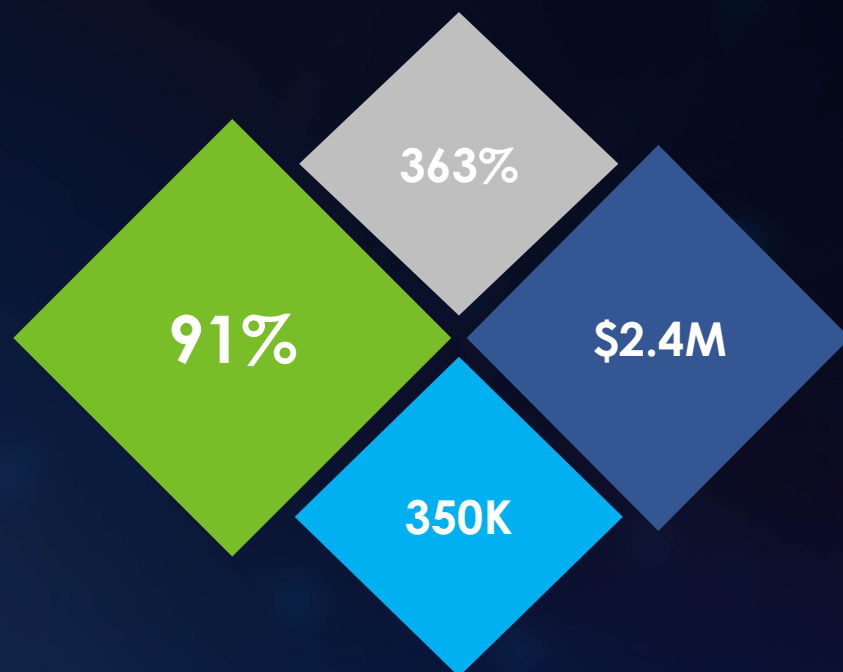
The Future of Endpoint Security



PART 1

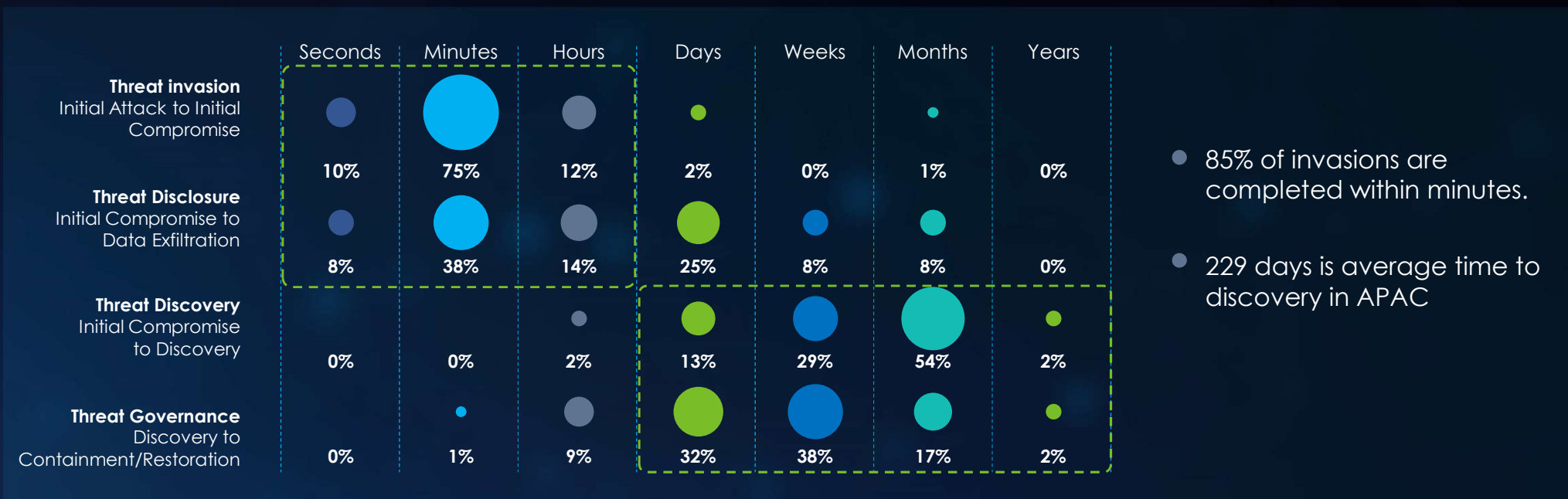
The Threat

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



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



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Outdated Defence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

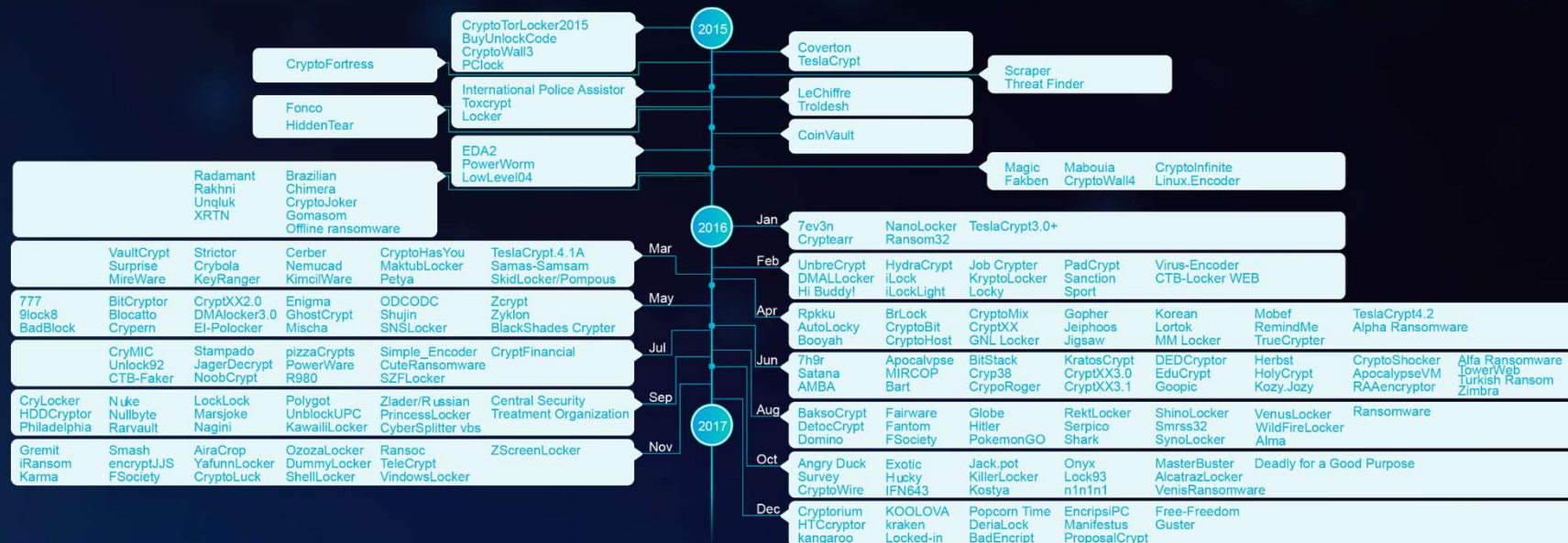
Ransomware Bypasses Traditional & Next Gen Antivirus



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

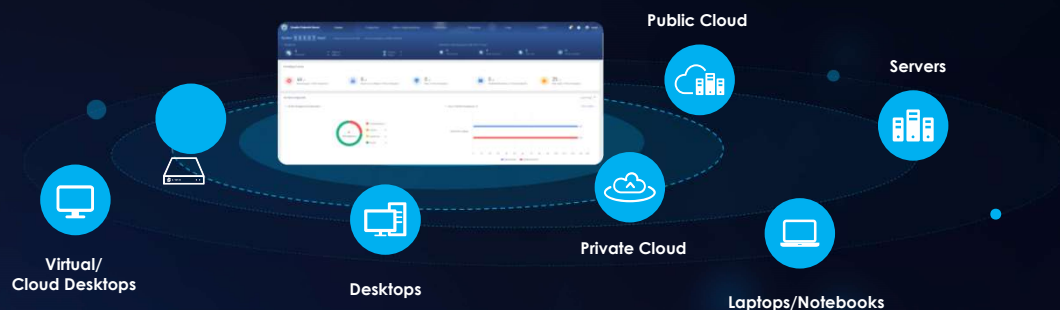
Continuous Evolution of Capabilities
Using Cloud-Based TI & AI

Security Operations
Managed Service



Endpoint Secure

The Future of Endpoint Security



Enterprise Asset Integration Strategy

Operating Systems



Virtualization



A Different Approach
For Defending Endpoints



AI powered protection
using Neural-X and
Engine Zero

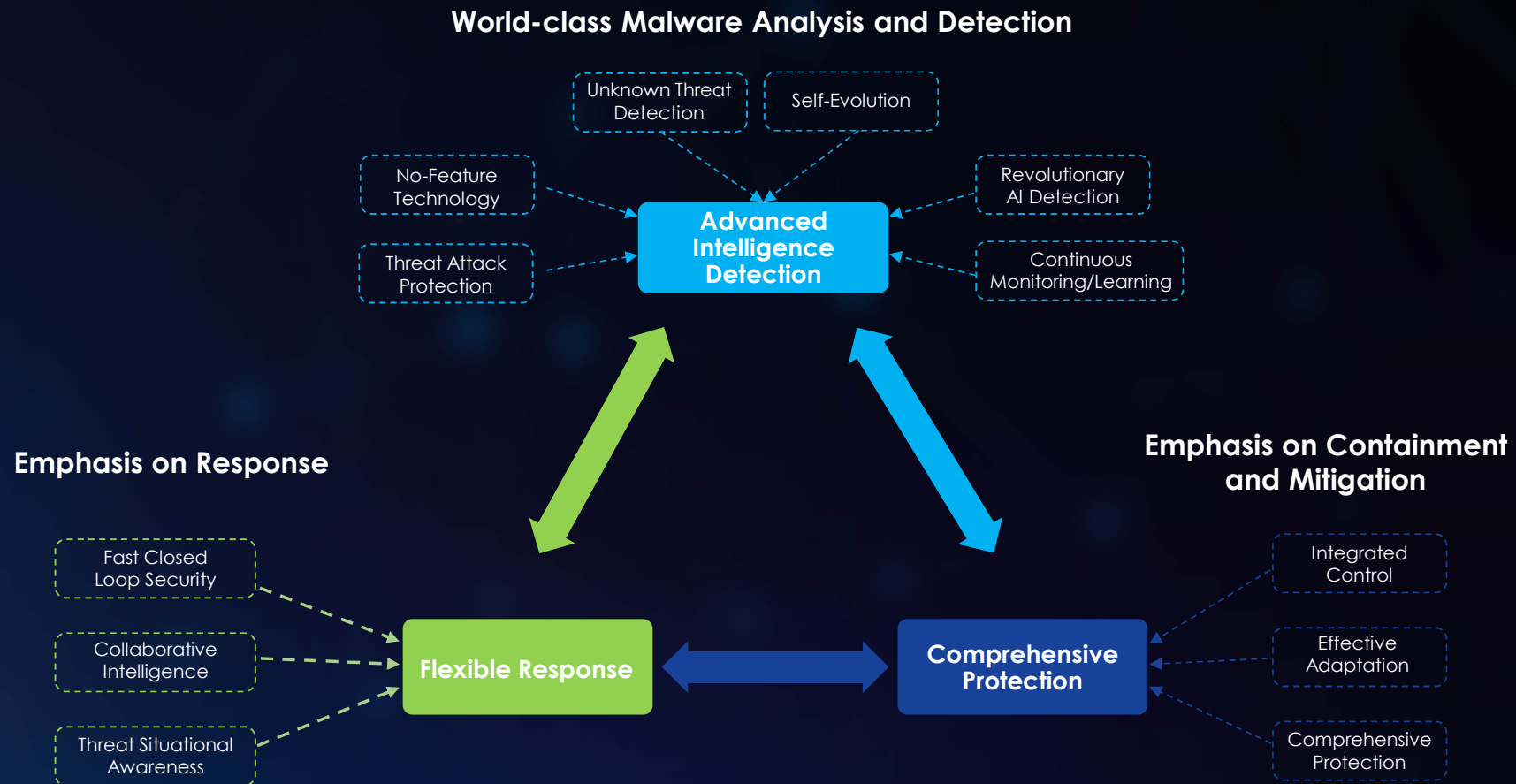


On-premise, Cloud-based
or Hybrid Management for
Scalability

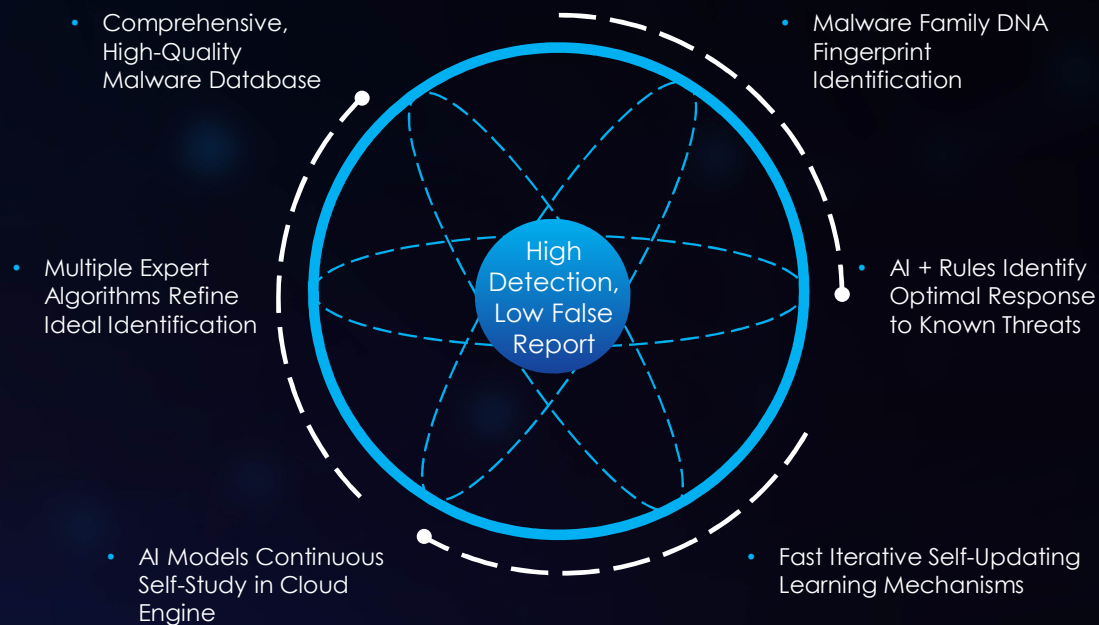
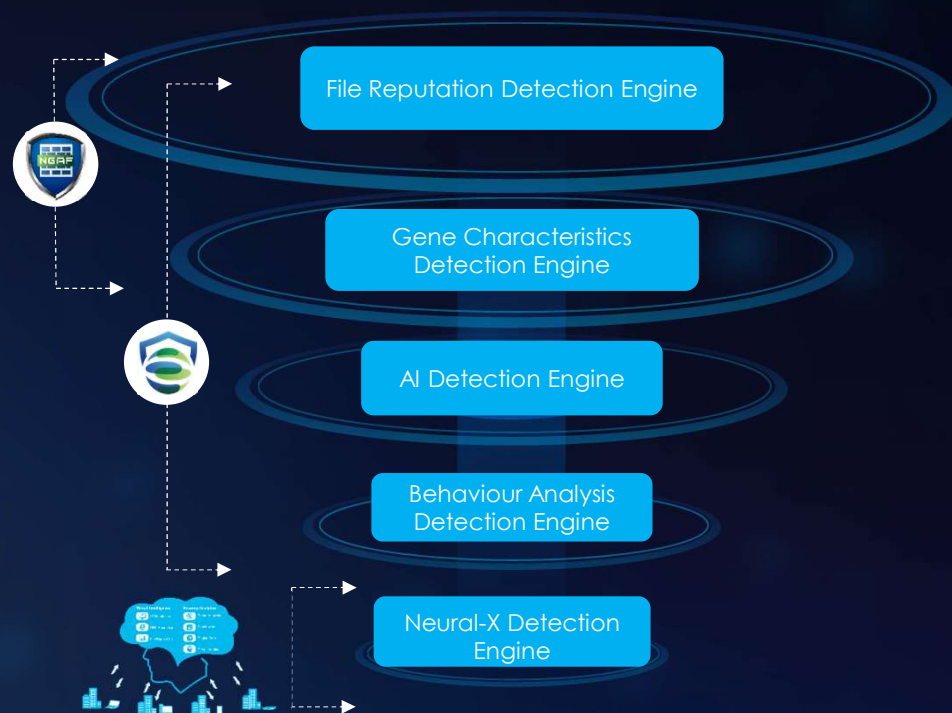


Direct Integration with
Sangfor NGAF

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

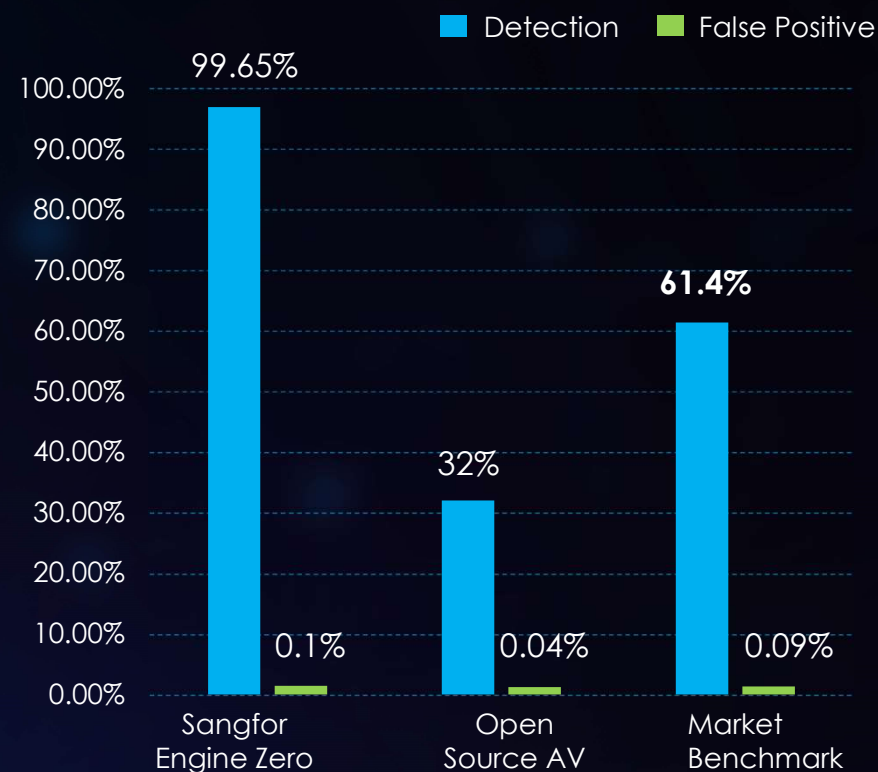
99.65% Accuracy with Unknown Malware Detection

>99.9% Accuracy with Known Malware Detection

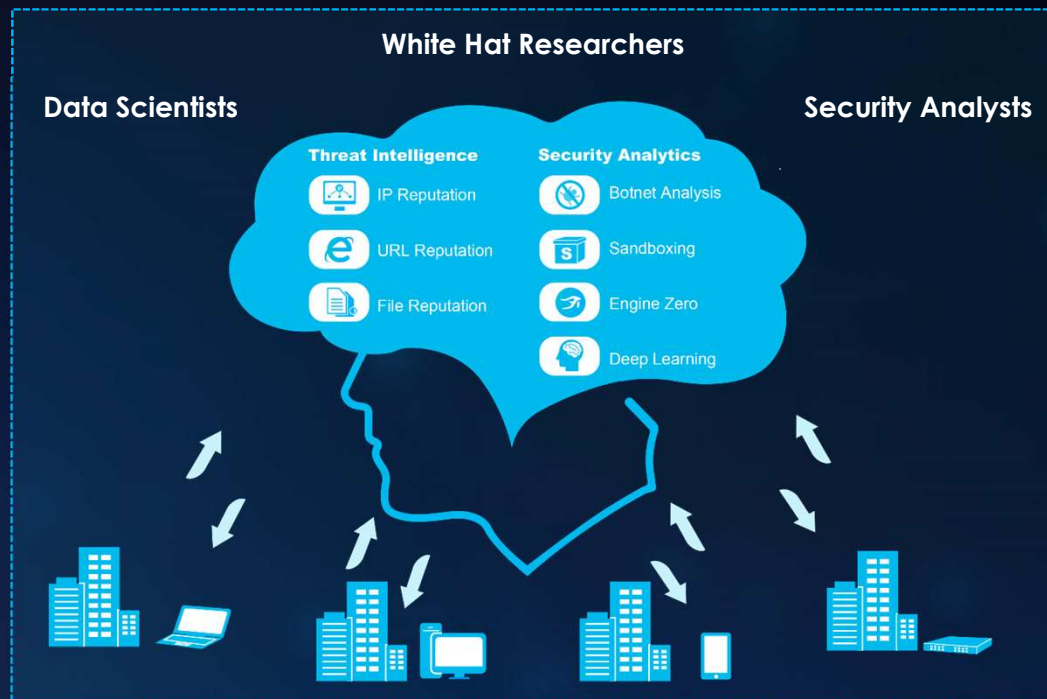


Globelmposter Ransomware

Zero-Day Detection



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

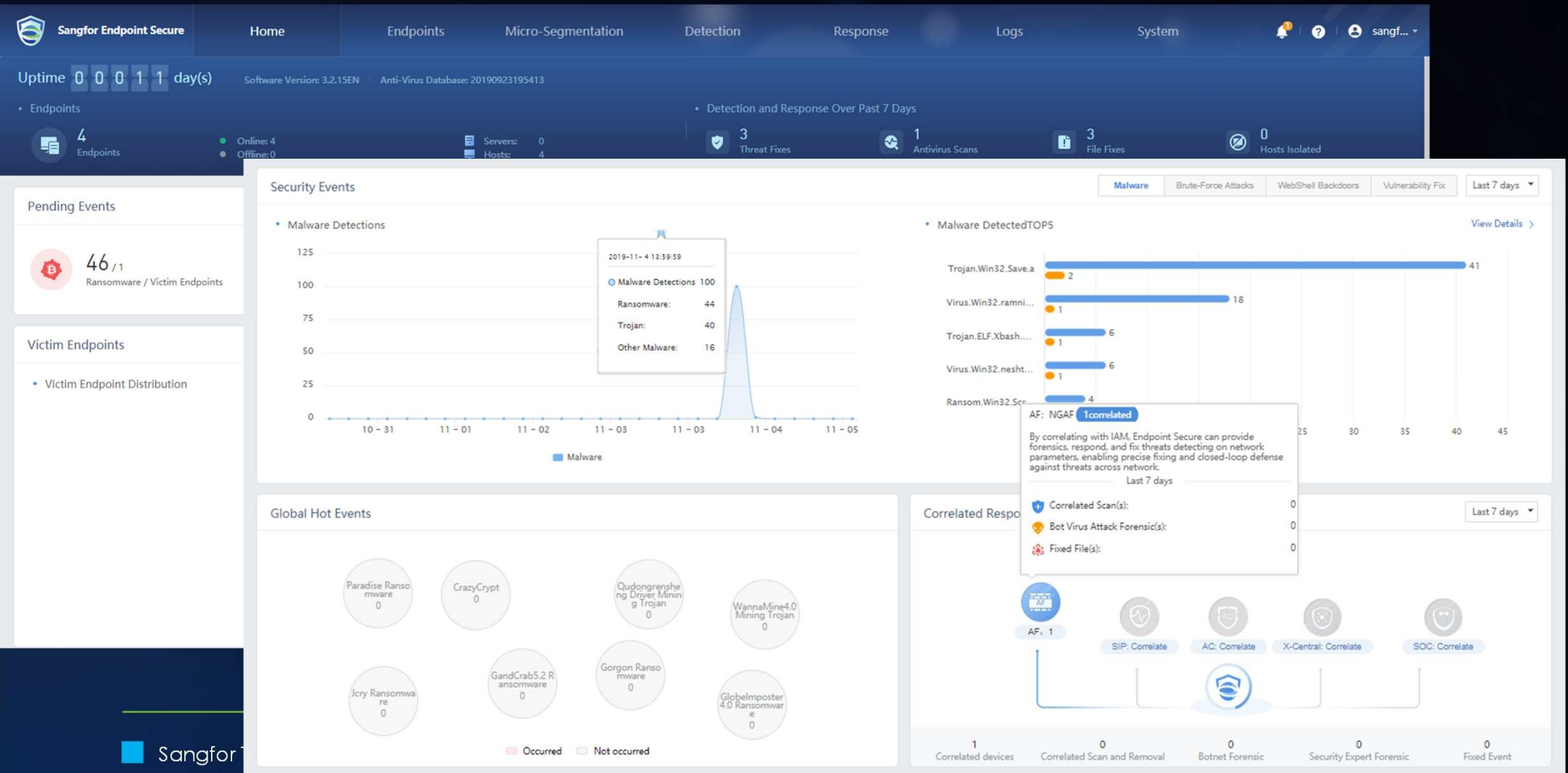


- Real-Time Unknown Threat Detection
- Cloud Sandbox
- Fast Response
- 30K Devices Share Intelligence
- 33 Billion Requests/day
- 60+ Countries

Multi-Dimensional Response



Security Visibility

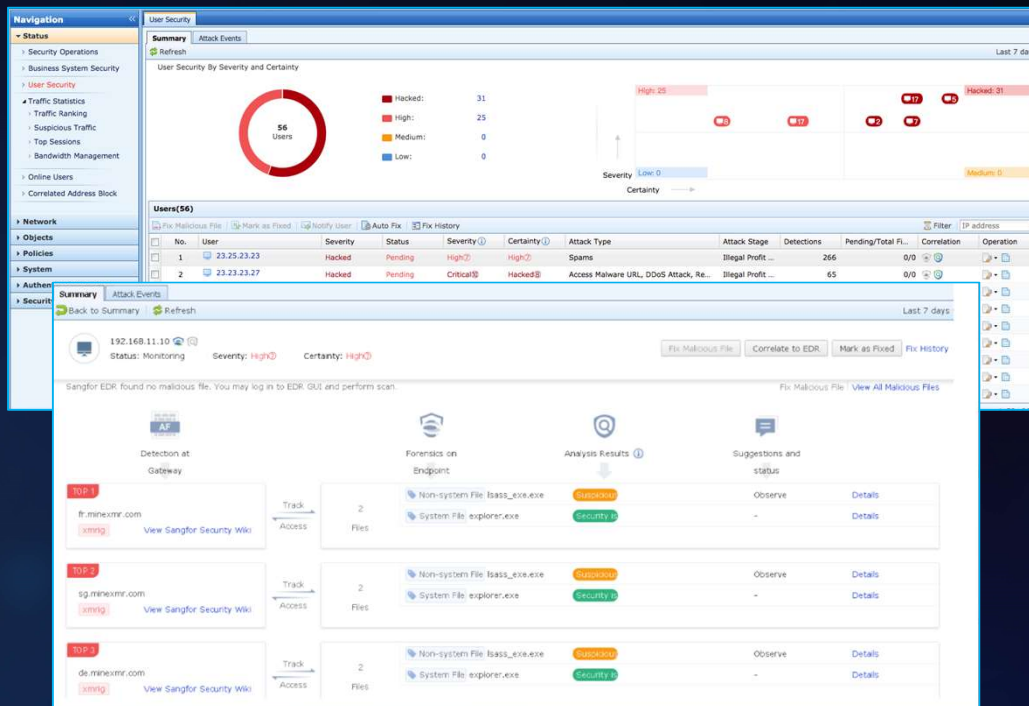


Detection

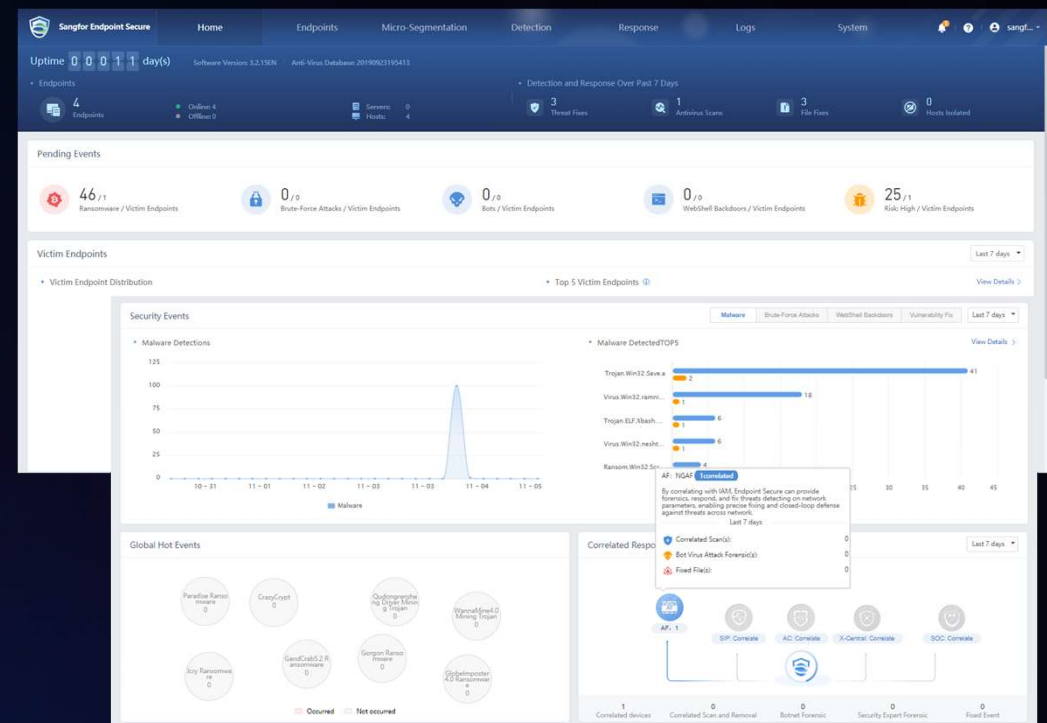


Risks to both PCs and servers are visible

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

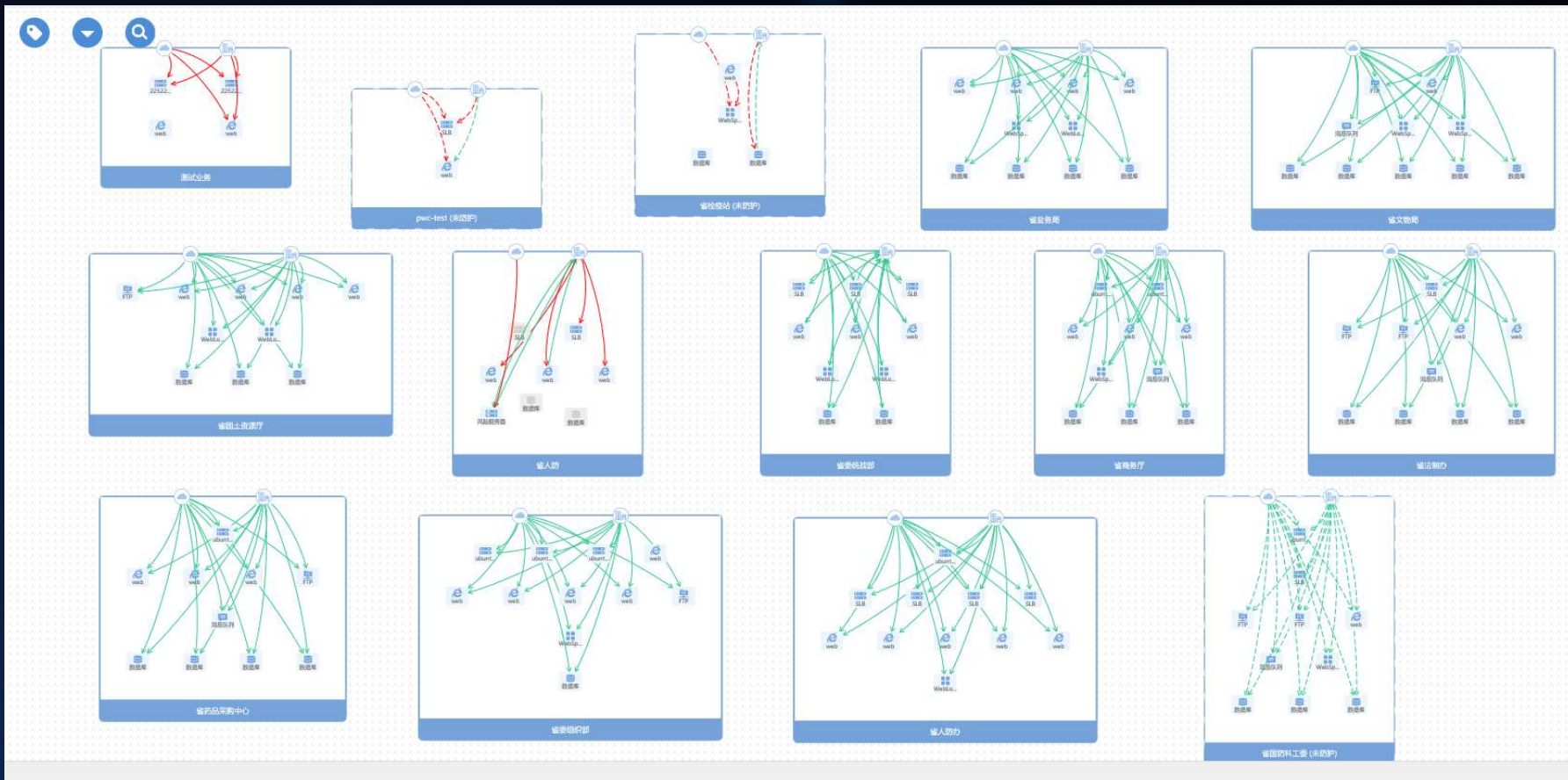
Identify vulnerabilities and risks to business assets



Visibility of Asset Behavior

Distinguish between common and uncommon asset behavior

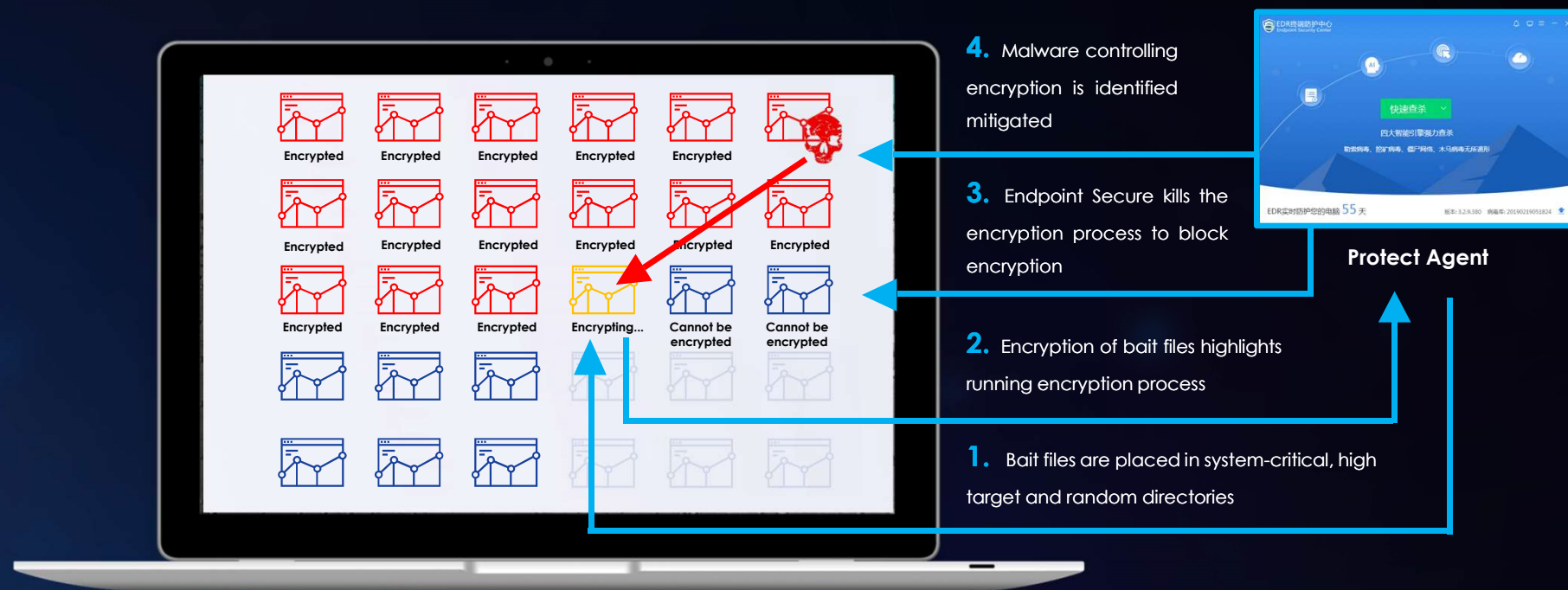
Identify Communications Between Endpoints



Ransomware Honeypot



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



Multi-Dimensional Response



Response



Sangfor Endpoint Secure

Home

Endpoints

Micro-Segmentation

Detection

Response

Logs

System

🔔

?

👤 sangf...

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: 4EE6E11350544F1A5C5EAF628DE25D8

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

c:\users\86156\desktop\af... .zip

c:\users\86156\desktop\...7e179d6

c:\users\86156\desktop\...6d6692f

c:\users\86156\desktop\...7c3dc9a

c:\users\86156\desktop\...6e7332f

c:\users\86156\desktop\...4f358b4

c:\users\86156\desktop\...4e937b8

c:\users\86156\desktop\...8e0e91fd7ee9ff25d80c...

c:\users\86156\desktop\...4adf99444453e5a3ece...

c:\users\86156\desktop\...3b42f1f73c73ed8aaec...

2019-09-23 03:30:18

2019-09-23 03:30:18

2019-09-23 03:30:18

Pending

Pending

Pending

Fix

Fix

Fix

Threat Intelligence

Threat Intelligence

Threat Intelligence

46 entries

<<

<

1

2

3

4

5

>

>>

Entries Per Page 10

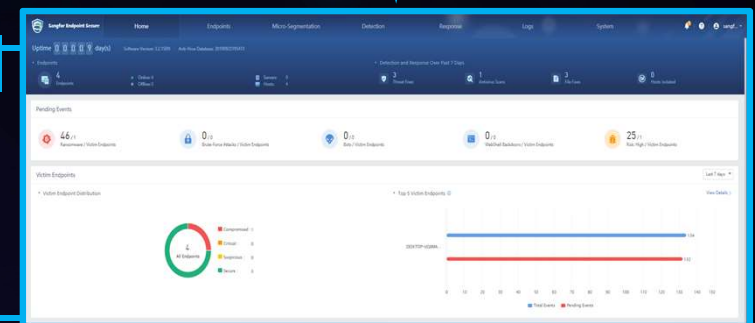
One-Click Kill



Find one infection, quickly scan the network for more

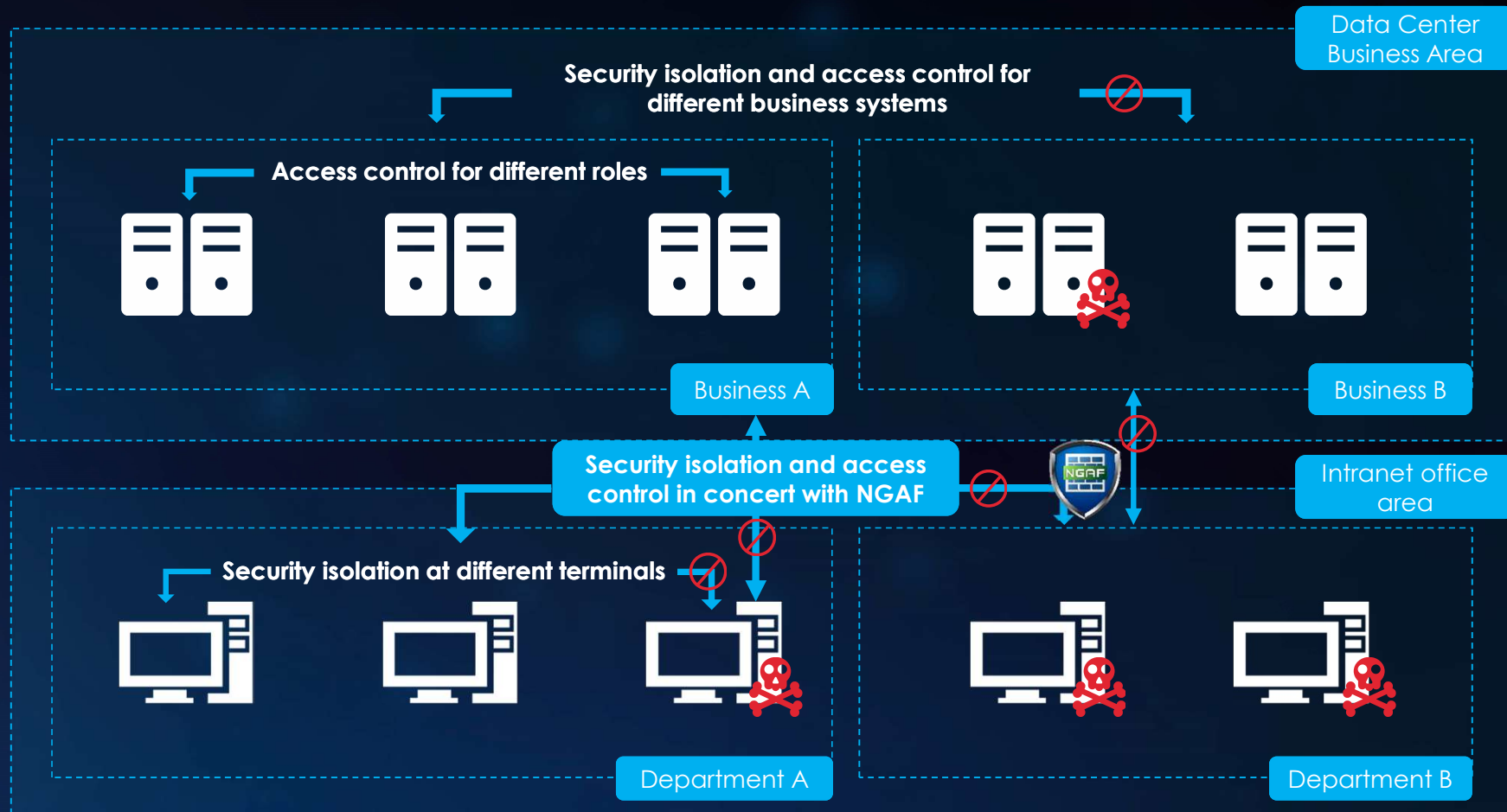
One click mitigation for the entire network

One click mitigation for the entire network

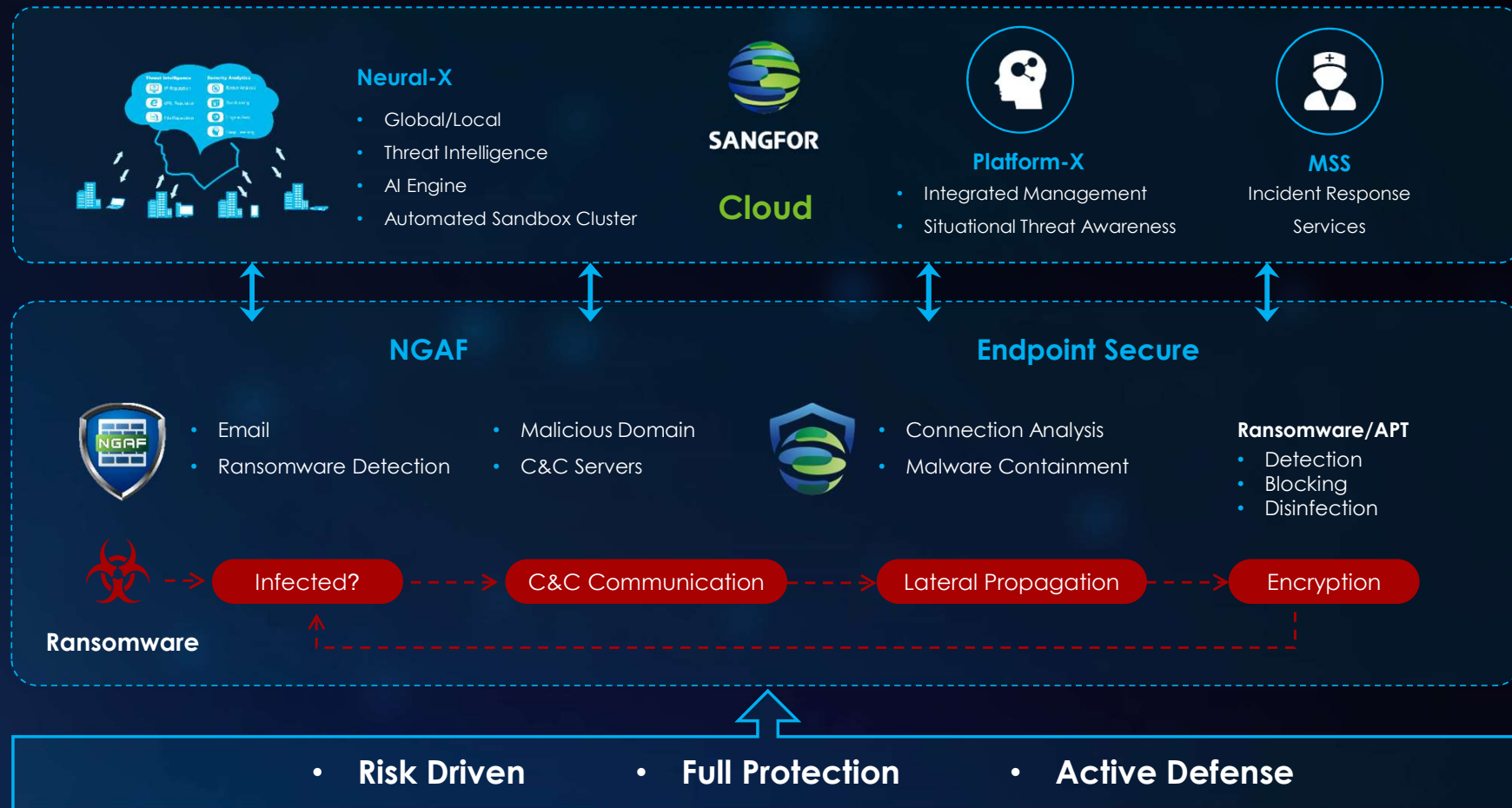


Endpoint Secure Manager

Micro-isolation reduces threat propagation



Risk Protection for Ransomware



Simplified Security Operation



Details(DESKTOP-UQ8MAR1, 172.16.244.175)

No.	Infected File/Process	Security Events	Time Detected	Status	Operation
1	c:\users\86156\desktop\...	Virus Name: UNQ/Safegit.spd	2019-09-25 03:20:05	Pending	Fix
2	c:\users\86156\desktop\...	Virus Name: UNQ/Safegit.WI	2019-09-25 03:20:05	Pending	Fix
3	c:\users\86156\desktop\...	Virus Name: UNQ/Safegit.pseur	2019-09-25 03:20:05	Pending	Fix
4	c:\users\86156\desktop\...	Virus Name: UNQ/Safegit.Bath	2019-09-25 03:20:05	Pending	Fix
5	c:\users\86156\desktop\...	Virus Name: UNQ/Safegit.Juba	2019-09-25 03:20:05	Pending	Fix
6	c:\users\86156\desktop\...	Virus Name: Ransom.Win32.Black...	2019-09-25 03:20:16	Pending	Fix
7	c:\users\86156\desktop\...	Virus Name: Ransom.Win32.Black...	2019-09-25 03:20:16	Pending	Fix
8	c:\users\86156\desktop\...	Virus Name: HEUR/AGEN.1020119	2019-09-25 03:20:16	Pending	Fix
9	c:\users\86156\desktop\...	Virus Name: Trojan.Win32.Sam...	2019-09-25 03:20:16	Pending	Fix
10	c:\users\86156\desktop\...	Virus Name: Trojan.Win32.War...	2019-09-25 03:20:16	Pending	Fix

Fix

Are you sure that you want to Fix the threat (c:\users\86156\desktop\...) on endpoint DESKTOP-UQ8MAR1 (172.16.244.175)?

☐ Also Fix file with same MD5 on other endpoints

OK Cancel

Message

Are you sure that you want to isolate DESKTOP-UQ8MAR1 (172.16.244.175, 200.200.120.228)?

Isolated endpoints will not be reachable to any network but still can be restored. Please assess the impacts to your business system.

OK Cancel

One Click Mitigation

Scan Task

Task Details

No.	Status	Severity	Threat Name	Group	IP Address	OS	Total Value	Unpatched Value	Operation
1	Completed	High	2019-09 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4516065)	Unpatched Endpoints	172.16.18.24	Windows 7 Professional Service...	25	25	Fix

EDR-NEW0083

No.	Severity	Type	Patch Name	Patch ID	Date Released	Status
1	High	Information Disclosure	2019-09 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4516065)	KB4516065	2019-09-09	Pending
2	High	Information Disclosure	2019-09 Security Only Quality Update for Windows 7 for x64-based Systems (KB4516033)	KB4516033	2019-09-09	Pending
3	High	Tampering	2019-08 Security Only Quality Update for Windows 7 for x64-based Systems (KB4512486)	KB4512486	2019-08-10	Pending
4	High	Remote Code Execution	2019-01 Security Only Quality Update for Windows 7 for x64-based Systems (KB4480960)	KB4480960	2019-01-04	Pending

Details

Patch ID: KB4516065 **High**

Patch Name: 2019-09 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4516065)

Description: A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.

Type: Information Disclosure **Restart to Apply**

Released On: 2019-09-09

Download: <http://download.windowsupdate.com/d/msdownload/update/software/secur/2019/09/windows6.1-kb4516065-x64-fbc436f2c56af4ab270e2d1b17b11a119265e904.cab>

Close

Vulnerability Scan with Remediation

Sangfor Endpoint Protection

Home

Summary

45% Malicious Endpoints

0% Suspicious Endpoints

0% Malicious Endpoints

25% Suspicious Endpoints

Security Events

Malicious

0d66302cb91b43924314c439265cb61

Virus name: Trojan.Linux.GaigeLab

File Type: FAT_AJG

File size: 100241

Found time: 2019-04-25 11:05:14

Updated: 2019-09-25 04:33:32

MD5: 0d66302cb91b43924314c439265cb61

SHA1: Unknown

SHA256: Unknown

IOC event: unknown

Related security incidents: No related events

Impact Analysis

Product Inspection

32 Total product counts

Customer Inspection

9 Number of customers

Influence Industry TOP5

No relevant data yet

Informative Visual Dashboard & TI

Endpoint Secure Requirements

The Future of Endpoint Security



Enterprise Asset Integration Strategy



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



THANK YOU

