SANGFOR

Comprehensive Ransomware Protection

Boo Soon Fatt | Presales Manager
Sangfor Technologies

Company Profile

SANGFOR

New HQ in Shenzhen, China

- **Global** network security & cloud computing provider.
- **Founded** in 2000, headquartered in Shenzhen, China with 60+ branches worldwide.
- **Local market presence** since 2010.
- **Team** with nearly 10,000 employees globally.
- **CMMI Level 5 Certified R&D.**
- **World's First 3rd Gen HCI.**
- **World's First Converged Firewall + WAF.**
- **Own Applied Patents** over 2,000+.
- **Recognized** in Gartner Magic Quadrant, Cyber Ratings, Forrester.

Global Expansion

60+ Global Branches

Sangfor Malaysia Office

- **Established in 2010**
- **3 Office in KL:** Sales, Call Centre and SOC
- **Team with 80+ employee**

Remote Tech with 24/7 Support

Multilingual Call Center in Malaysia

Sangfor Solution Portfolio

SANGFOR

Network Security & Optimization

1. **NSF/SDWAN** - Next Generation Application Firewall
2. **ES –** EDR
3. **IAG** - Internet Access Gateway
4. **Cyber Command** - NDR
5. **Omni-Command** - XDR
6. **SASE** – Secure Access Service Edge

Cloud Computing

1. **HCI** – Hyper Converged Infrastructure
2. **VDI** – Virtual Desktop Infrastructure
3. **MCS** – Managed Cloud Service
4. **aStor** – Enterprise Storage Solution

Security Services

1. **Cyber Guardian** – MDR
2. **TIARA** – Threat Intelligences, Analysis and Risk Assessment
3. **IR** – Incident Responses

Sangfor Customers in Malaysia

SANGFOR

Government/GLC

MAMPU BERSAMA-SAMA MELAKSANAKAN TRANSFORMASI

SPA SURUHANJAYA PERKHIDMATAN AWAM

MOSTI KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

JPJ JABATAN PENGANGKUTAN JALAN MALAYSIA

POLIS DIRAJA MALAYSIA

Air Selangor

Education

UNIVERSITI MALAYSIA SARAWAK UNIMAS

UNIVERSITI TEKNOLOGI MARA

UNIVERSITI KEBANGSAAN MALAYSIA The National University of Malaysia

UNISZA UNIVERSITI SULTAN ZAINAL ABIDIN

UPM UNIVERSITI PUTRA MALAYSIA BERILMU BERBAKTI

UUM Universiti Utara Malaysia

Healthcare

HOSPITAL PUTRAJAYA

TOGETHER FOR EXCELLENCE HOSPITAL SEREMBAN

HRPB HOSPITAL RAJA PERMAISURI BAINUN, IPOH KAMI ENDAH

PUSAT PERUBATAN UNIVERSITI MALAYA

HOSPITAL SUNGAI BULOH

PANTAI HOSPITAL Kuala Lumpur

Enterprise

ViTrox

YTL CEMENT

SONY

P&O PACIFIC & ORIENT INSURANCE CO BERHAD

HITACHI Inspire the Next Hitachi Sunway Information Systems

SILTERRA

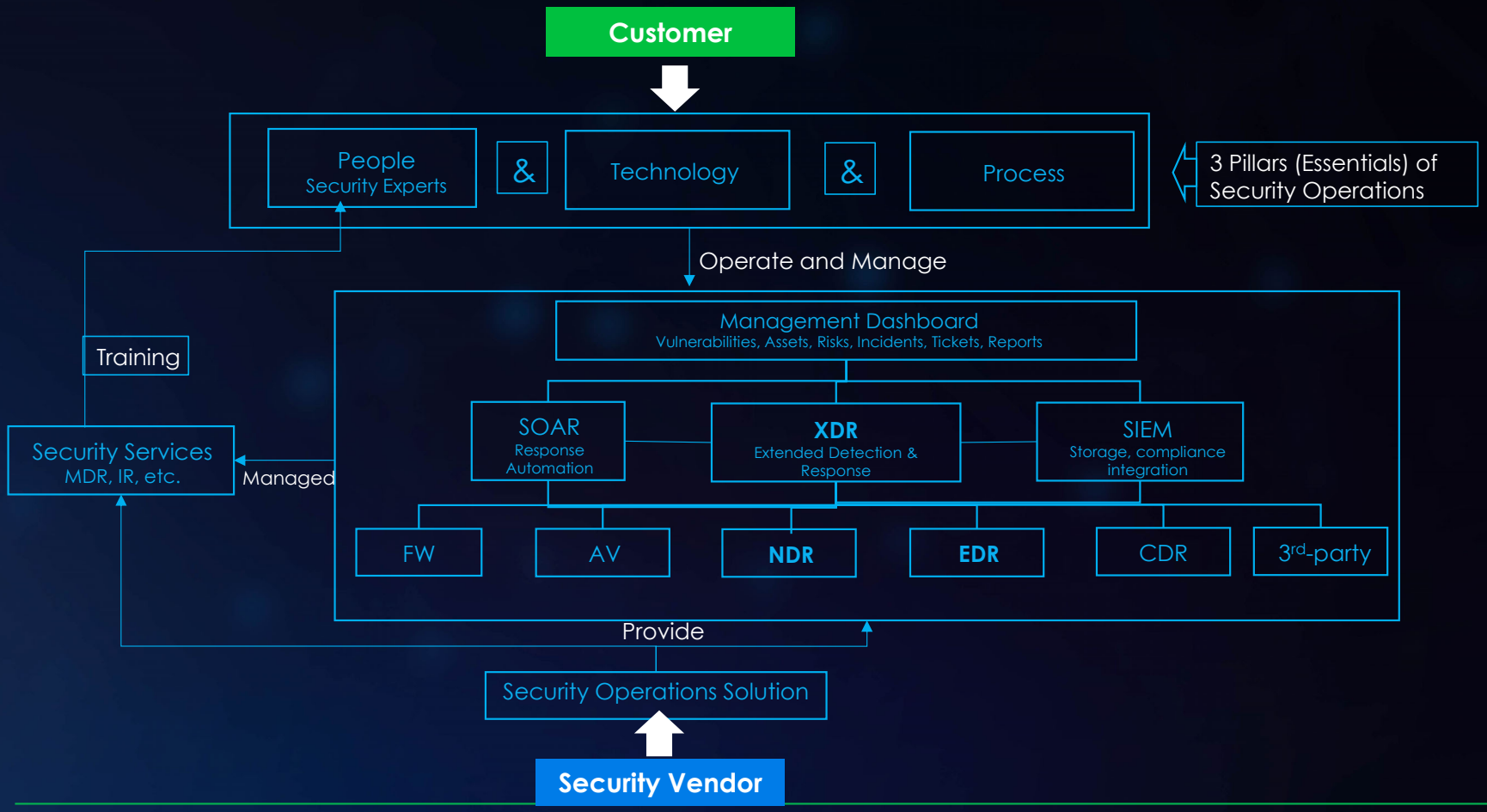
Contents

PART 1

The Need for Security Operations

Organizational Cyber Security Challenges

Security Operation



Cybersecurity Challenges in Organization

SANGFOR

Lack of Security Network

There are many branches access headquarters business through public network, The network lacks unified management and branches lack security construction

Lack of Systematic Security construction

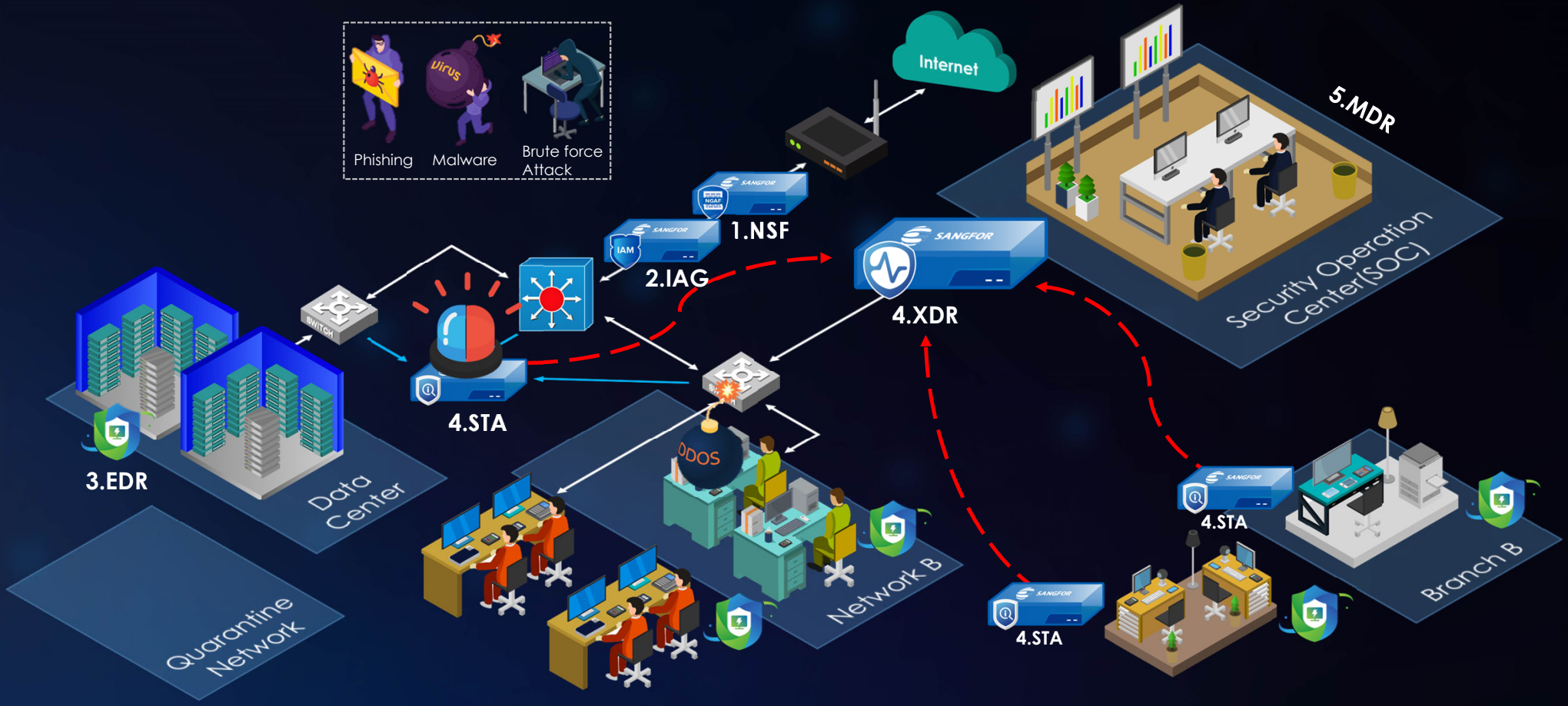
Just stacking security devices at the network boundary, unable to have the ability to specifically protect against ransomware.

Lack of Useful Backup

The business is relatively decentralized, and many businesses cannot be managed as a whole
Lack of effective disaster recovery system construction

Build network security system, Build a trusted and secure network
Build a reliable business system

Sangfor Security Ecosystem



PART 2

Introduction to Endpoint Secure (EDR)

Different Positionings of Endpoint Security

AV

Anti-Virus
Compares suspicious file against known malware databases

NGAV

Next Generation Anti-Virus with advanced features like behavior analysis and AI capability

EDR

Endpoint Detection & Response
Detects and responds to breaches after occurrence

EPP

Endpoint Protection Platform
Multi-layered solution with prevention and advanced capabilities including EDR and management features

Sangfor Endpoint Secure Positioning

SANGFOR

Modern EPP

Prevention (AV/NGAV)

Block and kill malicious processes and files

Detection and Response (EDR)

Investigate and remediate suspicious activities that are not blocked

Endpoint Management

Management and reporting of endpoint systems

Sangfor Endpoint Secure

- Real-time scanning
- AI-enabled detection engines
- Fileless and in-memory exploit protection
- Ransomware Protection and Data Recovery
- APT detection and kill-chain analysis
- File quarantine and deletion
- Endpoint isolation
- MITRE ATT&CK mapping
- Phishing detection with auto - response
- Asset Inventory and Management
- Vulnerability Management
- App Control
- Remote support
- Logging and reporting

The Ideal Approach to Protect Endpoints

Attack Surface Reduction

Asset & Configuration Security / Vulnerability & Patch Management

- Real-time File Scanning
- Lightweight Scanning
- ML Detection for Static File
- Trusted Processes
- Key Directory Protection

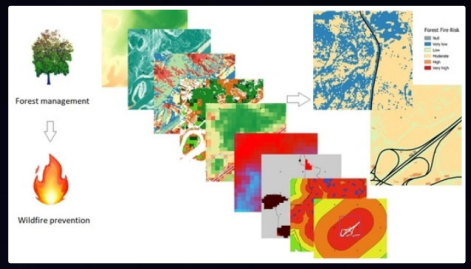
Pre-Execution

Signatures and ML for Static File Analysis

- ML Detection for Dynamic Behavior
- Honeypot for Deception
- Fileless Attack Protection
- Web Shell Protection
- RDP Secondary Authentication
- Brute-Force Attack Detection

Peri-Execution

Dynamic Behavior Analysis Technologies like ML for Behavior-Detection and Deception



- APT Detection
- Threat hunting
- Integrate with Global TI and network
- One-Click Network-Wide Kill

Post-Execution

Detection and Investigation, Automated Response, and Integration with ecosystem

Endpoint Secure Overview

Enterprise Asset Integration Strategy

Operating Systems

Windows · Centos · Ubuntu · Red-Hat · SUSE · Debian · Oracle Linux

Virtualization

Sangfor HCI · VMware · Nutanix

Operating Systems Support

- Windows
- Linux
- Mac

Platform Support

- Physical machines
- Virtual machines

Capabilities

- All NGEP capabilities
- Vulnerability detection & remediation
- Ransomware Protection
- Security Compliance Check
- Threat analysis & hunting
- MITRE ATT&CK Framework
- Sangfor XDDR

High OS Compatibility

Support legacy OS including Window XP SP3 and Window Server 2003 SP2

Windows	macOS	Ubuntu	Redhat	CentOS	Debian	SuSE	Oracle Linux	Other
• Windows XP SP3 * • Windows 7 * • Windows 8 * • Windows 8.1 * • Windows 10 • Windows 11 • Windows Server 2003 SP2 * • Windows Server 2008 * • Windows Server 2008R2 * • Windows Server 2012 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.13 • macOS 10.14 • macOS 10.15 • macOS 11.x • macOS 12.x • macOS 13.x	• Ubuntu 10 • Ubuntu 11 • Ubuntu 12 • Ubuntu 13 • Ubuntu 14 • Ubuntu 16 • Ubuntu 18 • Ubuntu 20 • Ubuntu 22	• RHEL 5 • RHEL 6 • RHEL 7 • RHEL 8	• CentOS 5 • CentOS 6 • CentOS 7 • CentOS 8	• Debian 6 • Debian 7 • Debian 8 • Debian 9	• SUSE 12 • SUSE 11.X • SUSE 15.X	• Oracle Linux 5 • Oracle Linux 6 • Oracle Linux 7 • Oracle Linux 8 • Oracle Linux 9	• Red Flag Asianux Server 4 • NeoKylin 5 • NeoKylin 6 • NeoKylin 7 • KylinOS 4 • Ubuntu Kylin 18

The Ransomware Kill Chain

Infection → **C&C** → **Exploitation** → **Propagation**

1st Step:
Initial Access
- Phishing
- Malicious URL
- RDP Brute Force
- USB Drive

Social Engineering

2nd Step:
C2 Communication
- DGA
- Remote Installation
- Sensitive Info Lost

Encrypted C&C

3rd Step:
Encryption
- File Encryption
- Double Extortion

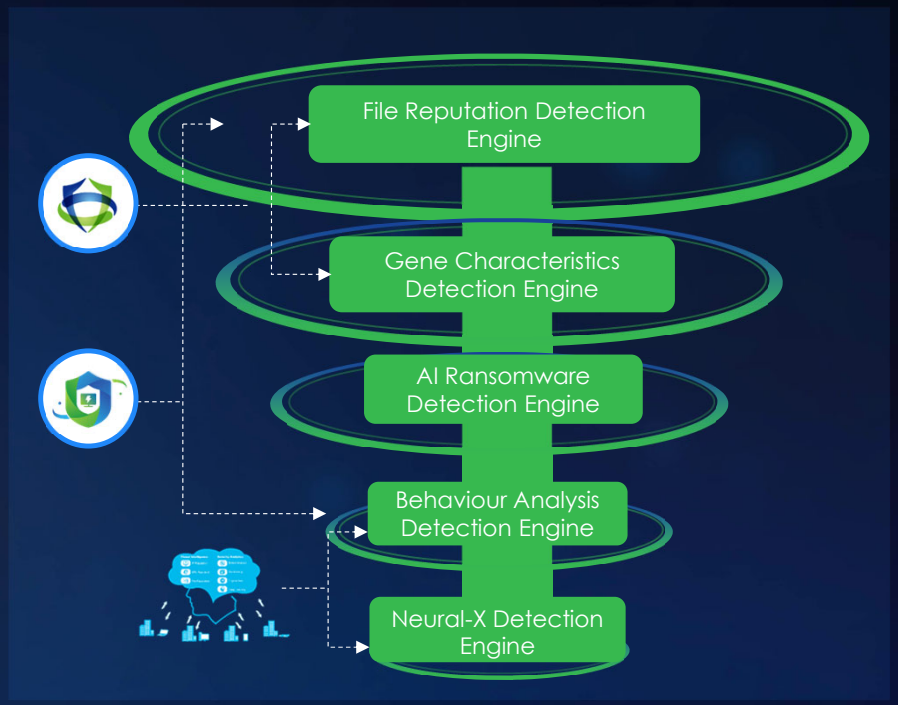
AI-Enabled Variants

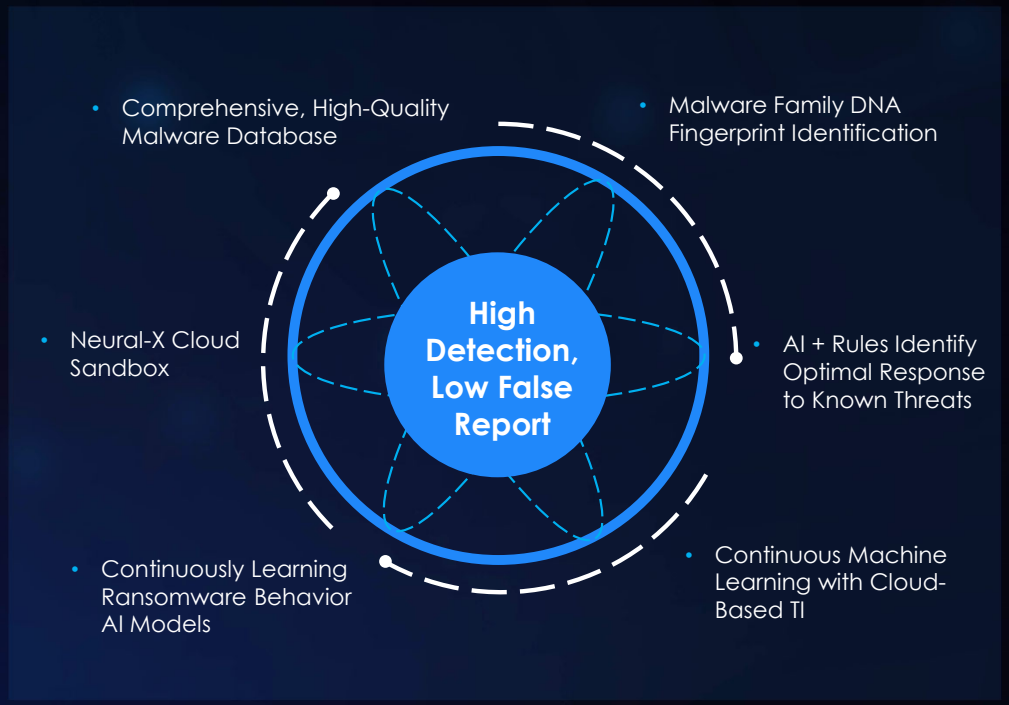
4th Step:
Horizontal Spread
- RDP Brute Force
- Worm
- System Vulnerability

Undetected Slow Scan

Once ransomware enters the internal network, it is 100% successful spreading horizontally in multiple directions in less than 45 minutes!

AI-Enabled Detection With Engine Zero





Ransomware Detection AI Models

Sangfor Engine Zero

AI Malware Detection Engine

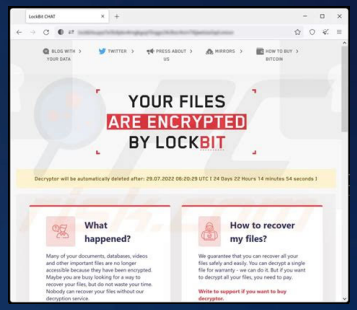
Innovative Unique AI Technology

High Detection Accuracy

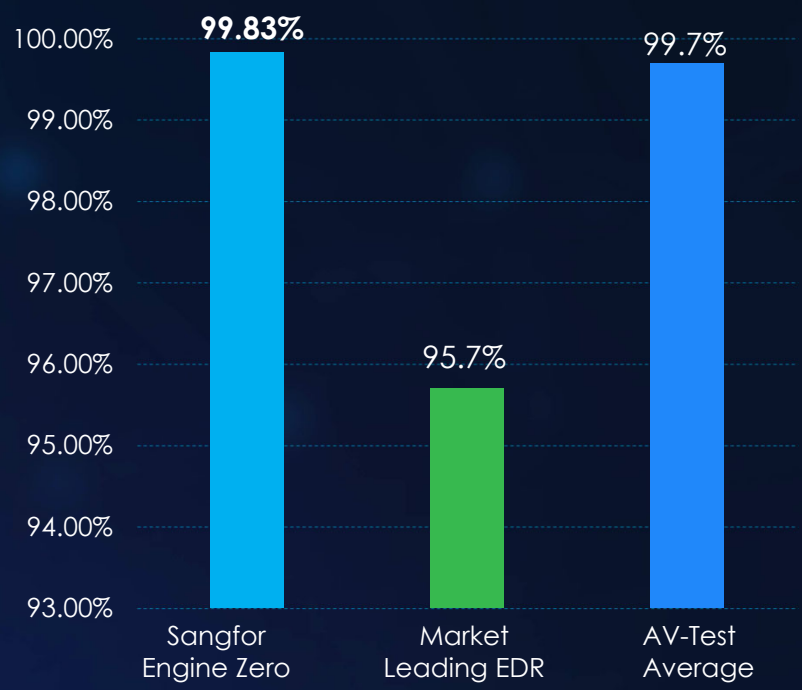
Low False Positive Rate

99.83% Accuracy for Unknown Ransomware Detection

100% Accuracy for Known Ransomware Detection



LockBit 3.0 Ransomware detected as zero-day

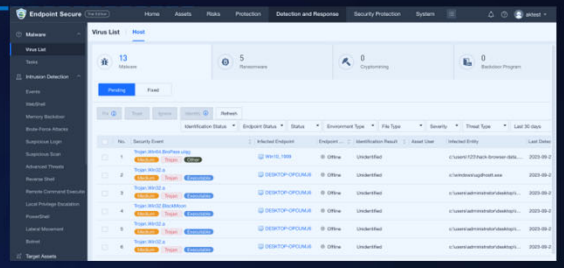


Synergy with Network Secure

SANGFOR

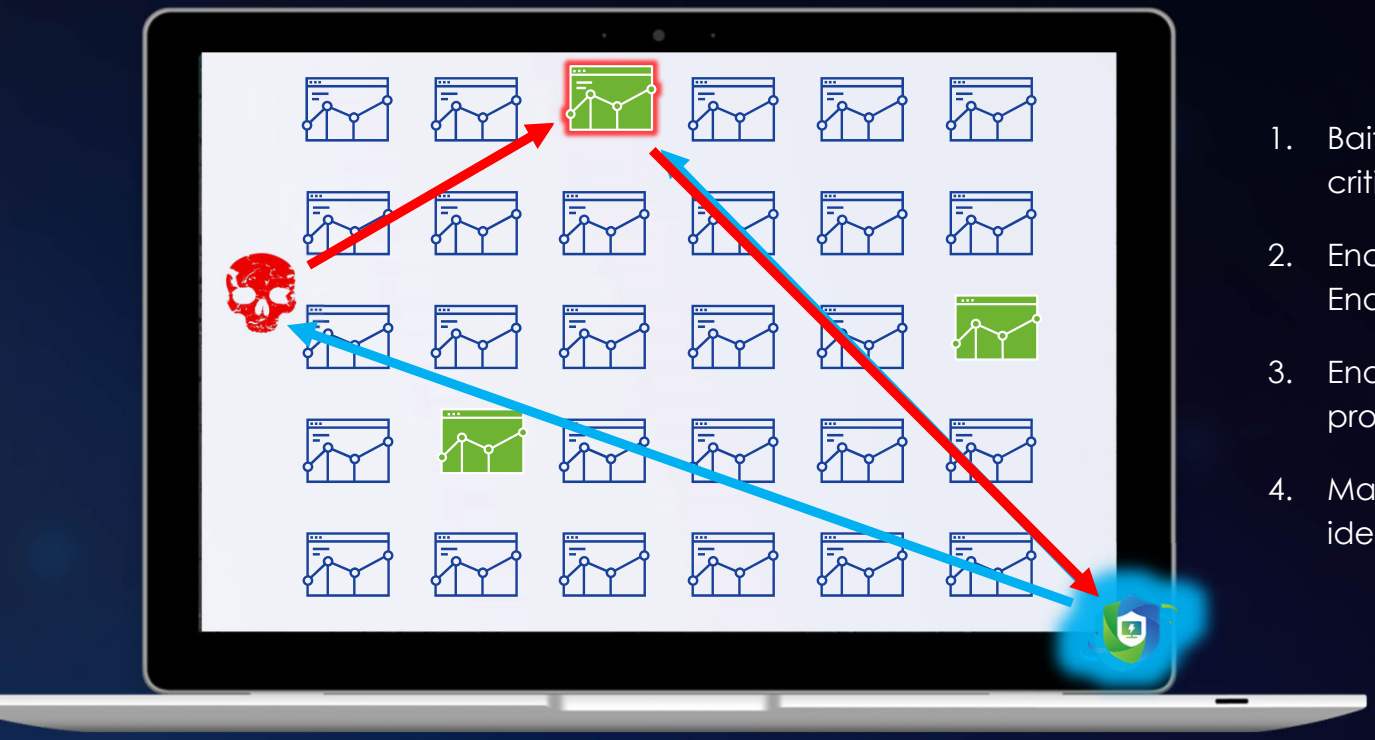
Ransomware → Infection → C&C → Exploitation → Propagation

Network Secure tells Endpoint Secure to run virus and vulnerability scans



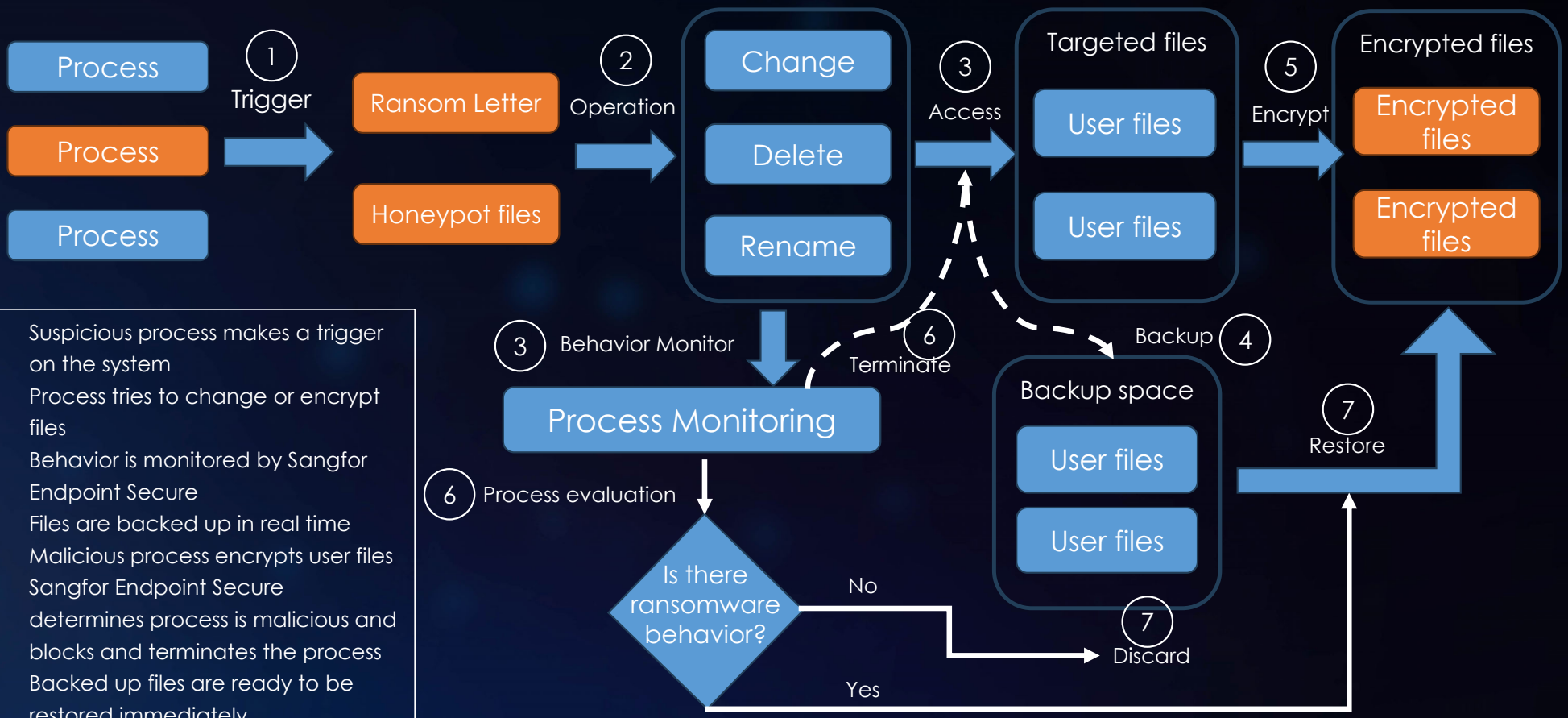
Stopping the Exploit - Ransomware Honeypot

Ransomware → Infection → C&C → Exploitation → Propagation



1. Bait files are strategically placed in system-critical, high-target, and random directories.
2. Encryption of bait files is detected by the Endpoint Secure agent.
3. Endpoint Secure agent kills the encryption process to block encryption.
4. Malware controlling the encryption is identified and mitigated.

Ransomware Protection and Recovery



1. Suspicious process makes a trigger on the system
2. Process tries to change or encrypt files
3. Behavior is monitored by Sangfor Endpoint Secure
4. Files are backed up in real time
5. Malicious process encrypts user files
6. Sangfor Endpoint Secure determines process is malicious and blocks and terminates the process
7. Backed up files are ready to be restored immediately

Ransomware Protection and Recovery Demo

Stopping the Exploit - One-Click Kill

1. MD5 hash of virus file is generated by Endpoint Secure file reputation engine.
2. Immediately distributed to other endpoints in the network.
3. Endpoint Secure manager instructs all agents to scan for the file and report back.
4. If found, endpoint will be added to "one-click" response for immediate and network-wide remediation.