Sangfor's Answer to Ransomware

When Ransomware Calls – Sangfor Answers

www.sangfor.com

SANGFOR

91% of cyber-attacks begin with a simple phishing email. Having a successful day phishing is easy, with new malicious malware samples produced daily, leading to a **363%** yearly increase in ransomware attacks. While cyber-phishermen aren't always successful, even one success could cost a company an average of **$2.4M.**

Huge Business impact
And Economic Loss
(Hard decryption)

About **350,000** new malicious
malware samples
are created everyday

Ransomware attacks within few
minutes but it normally takes
over **4 months** to discover

Ransomware has adapted to bypass traditional firewall security and even next generation anti-virus software with ease, as we saw when WannaCry brought **150** countries and **200,000** machines to their knees in only 4 days. It's an epidemic, and Sangfor has the cure.

Example of Recent Attacks

3rd August 2018

Company A was exposed to Ransomware (Wanna Cry)

- Industry: Manufacturing
- Loss: 2.60 billion USD
- Fortune Global 500: 300+

**Due to confidentiality issue, we are not allowed to divulge the customer name.*

August 2017

Company B was attacked by Ransomware (Petya)

- Industry: Shipping
- Loss: 270 million USD
- Fortune Global 500: 300+

**Due to confidentiality issue, we are not allowed to divulge the customer name.*

Why Do Ransomware Bypass Traditional Security Solution? 01

Most of the organizations only have a single security product protection mainly based on detection of MD5 signature. Low-detection rate for unknown threats.

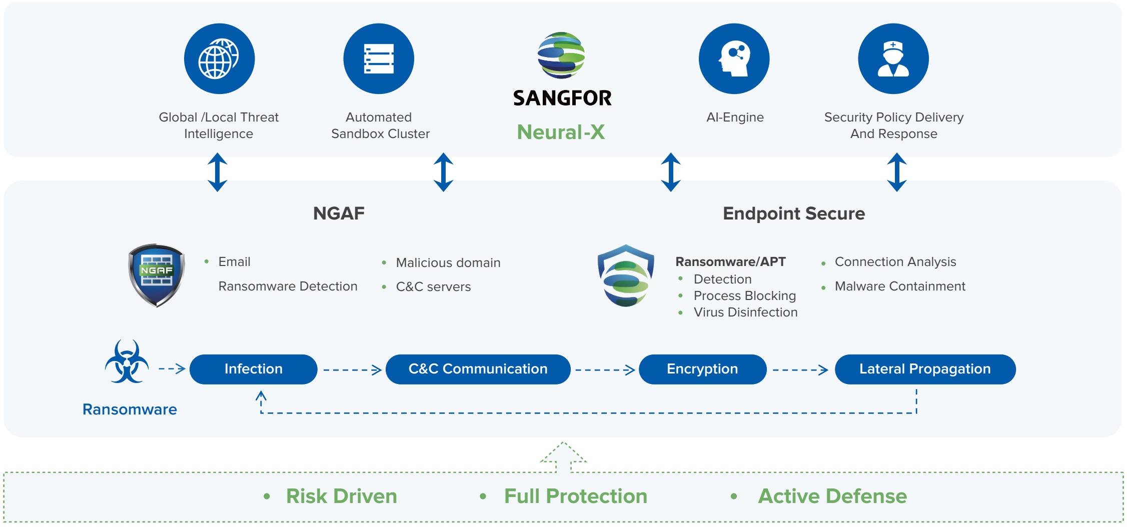
Traditional security solutions are based on the combination of multi-products rather than real cloud, network and endpoint correlation.

Sangfor Correlation Solution for Ransomware 02

A cocktail of Sangfor's NGAF, Endpoint Secure and Neural-X provide the risk-driven full protection and active defense against infection.

To be successful, ransomware must go through a full-attack cycle of infection, C&C communication, encryption and finally lateral propagation.

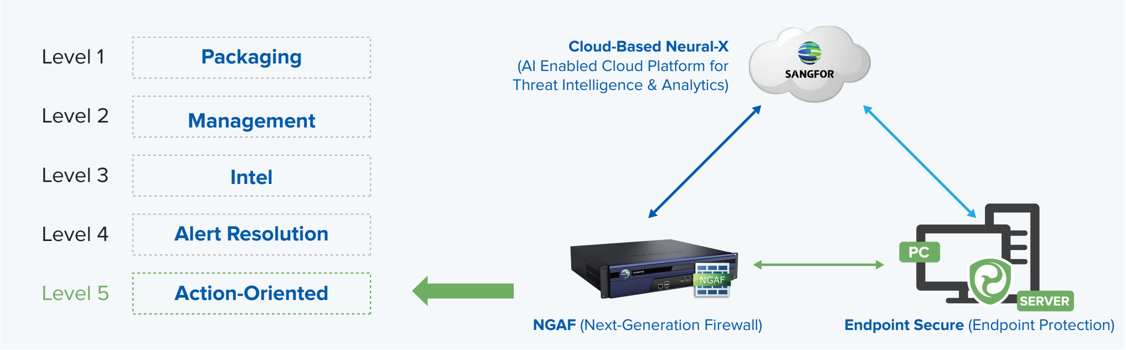
Neural-X is the brain's response to the ransomware attack, with global and local threat intelligence, automated sandbox cluster, AI-engine and security policy delivery & response. NGAF and Endpoint Secure work in tandem to provide the power of detection, analysis, blocking, containment and finally disinfection – giving users risk-driven, full protection and an active and vigorous defense.



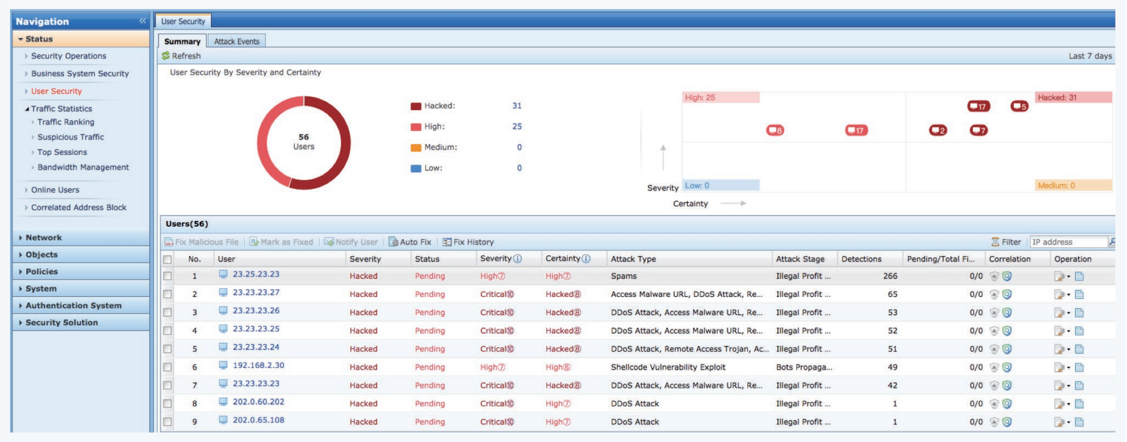
Solution Advantages 03

Leading Capability

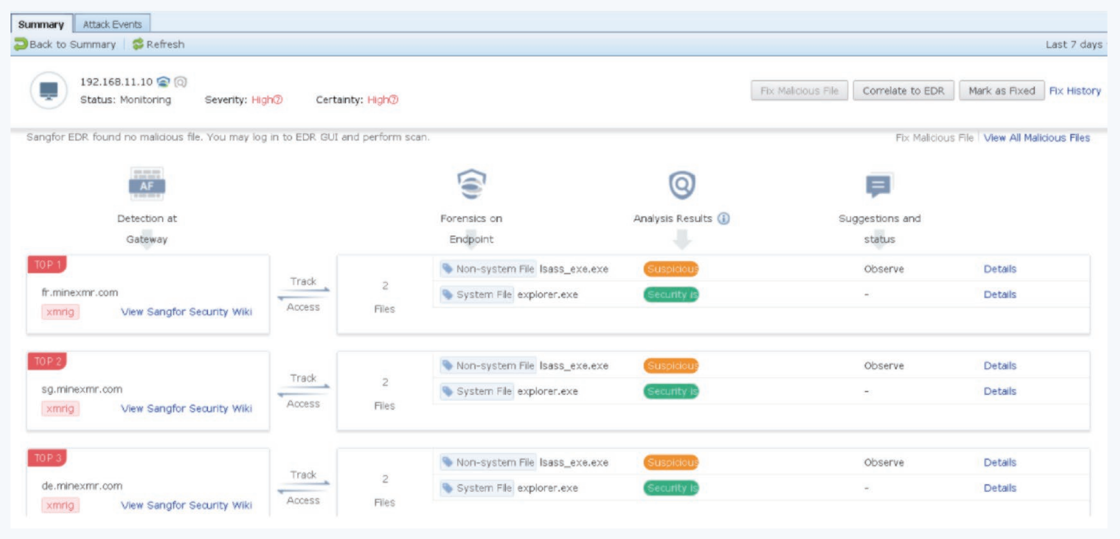
Gartner differentiates between security products with 5-levels of correlation – and Sangfor NGAF & Endpoint Secure occupy the top level of protection, security and safety.


Level 1
Packaging
Level 2
Management
Level 3
Intel
Level 4
Alert Resolution
Level 5
Action-Oriented
Cloud-Based Neural-X
(AI Enabled Cloud Platform for Threat Intelligence & Analytics)
SANGFOR
NGAF
PC
SERVER
NGAF (Next-Generation Firewall)
Endpoint Secure (Endpoint Protection)

Fully Visibility For PC And Server Threats In Single Platform



□	No.	User	Severity	Status	Severity	Certainty	Attack Type	Attack Stage	Detections	Pending/Total Fi...	Correlation	Operation
□	1	23.25.23.23	Hacked	Pending	High⑦	High⑦	Spams	Illegal Profit ...	266	0/0		
□	2	23.23.23.27	Hacked	Pending	Critical⑩	Hacked⑧	Access Malware URL, DDoS Attack, Re...	Illegal Profit ...	65	0/0		
□	3	23.23.23.26	Hacked	Pending	Critical⑩	Hacked⑧	DDoS Attack, Access Malware URL, Re...	Illegal Profit ...	53	0/0		
□	4	23.23.23.25	Hacked	Pending	Critical⑩	Hacked⑧	DDoS Attack, Access Malware URL, Re...	Illegal Profit ...	52	0/0		
□	5	23.23.23.24	Hacked	Pending	Critical⑩	Hacked⑧	DDoS Attack, Remote Access Trojan, Ac...	Illegal Profit ...	51	0/0		
□	6	192.168.2.30	Hacked	Pending	High⑦	High⑥	Shellcode Vulnerability Exploit	Bots Propaga...	49	0/0		
□	7	23.23.23.23	Hacked	Pending	Critical⑩	Hacked⑧	DDoS Attack, Access Malware URL, Re...	Illegal Profit ...	42	0/0		
□	8	202.0.60.202	Hacked	Pending	Critical⑩	High⑦	DDoS Attack	Illegal Profit ...	1	0/0		
□	9	202.0.65.108	Hacked	Pending	Critical⑩	High⑦	DDoS Attack	Illegal Profit ...	1	0/0		



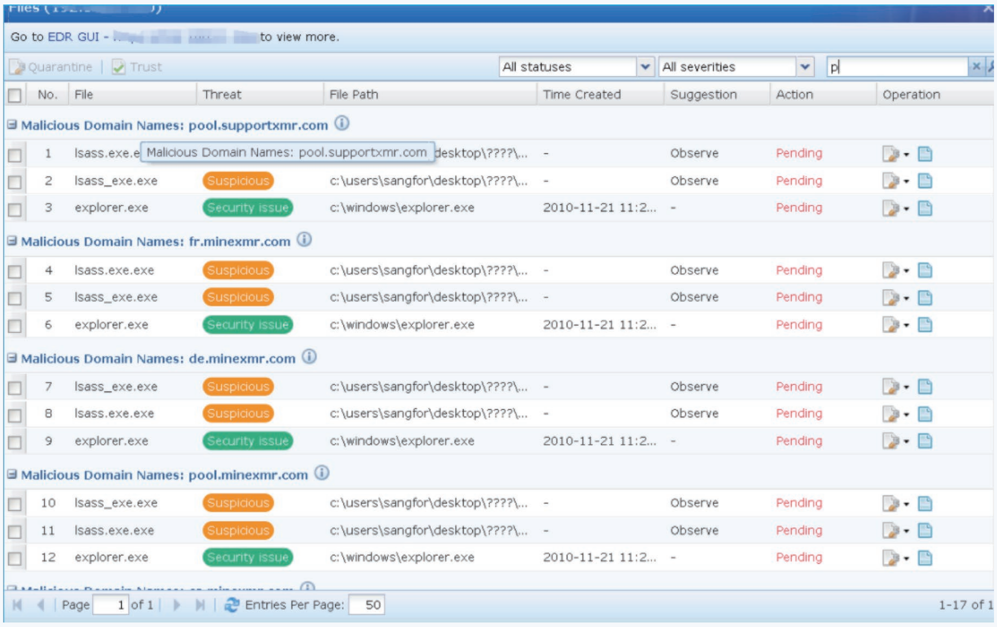
192.168.11.10

Status: Monitoring Severity: High Certainty: High

Sangfor EDR found no malicious file. You may log in to EDR GUI and perform scan.

Detection at Gateway		Forensics on Endpoint		Analysis Results	Suggestions and status	
TOP 1 fr.minexmr.com xmrig View Sangfor Security Wiki	Track Access	2 Files	Non-system File lsass_exe.exe	Suspicious	Observe	Details
			System File explorer.exe	Security is	-	Details
TOP 2 sg.minexmr.com xmrig View Sangfor Security Wiki	Track Access	2 Files	Non-system File lsass_exe.exe	Suspicious	Observe	Details
			System File explorer.exe	Security is	-	Details
TOP 3 de.minexmr.com xmrig View Sangfor Security Wiki	Track Access	2 Files	Non-system File lsass_exe.exe	Suspicious	Observe	Details
			System File explorer.exe	Security is	-	Details

Correlation Analysis and Traceability of Malicious Traffic & Endpoint Behavior

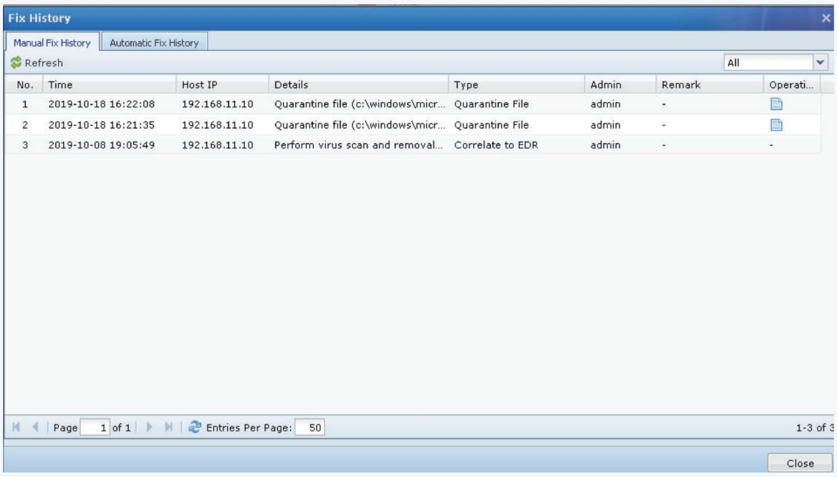


Go to EDR GUI - [redacted] to view more.

	No.	File	Threat	File Path	Time Created	Suggestion	Action	Operation
⊟ Malicious Domain Names: pool.supportxmr.com								
□	1	lsass.exe.e	Malicious Domain Names: pool.supportxmr.com	desktop\????\...	-	Observe	Pending	
□	2	lsass_exe.exe	Suspicious	c:\users\sangfor\desktop\????\...	-	Observe	Pending	
□	3	explorer.exe	Security issue	c:\windows\explorer.exe	2010-11-21 11:2...	-	Pending	
⊟ Malicious Domain Names: fr.minexmr.com								
□	4	lsass.exe.exe	Suspicious	c:\users\sangfor\desktop\????\...	-	Observe	Pending	
□	5	lsass_exe.exe	Suspicious	c:\users\sangfor\desktop\????\...	-	Observe	Pending	
□	6	explorer.exe	Security issue	c:\windows\explorer.exe	2010-11-21 11:2...	-	Pending	
⊟ Malicious Domain Names: de.minexmr.com								
□	7	lsass_exe.exe	Suspicious	c:\users\sangfor\desktop\????\...	-	Observe	Pending	
□	8	lsass.exe.exe	Suspicious	c:\users\sangfor\desktop\????\...	-	Observe	Pending	
□	9	explorer.exe	Security issue	c:\windows\explorer.exe	2010-11-21 11:2...	-	Pending	
⊟ Malicious Domain Names: pool.minexmr.com								
□	10	lsass_exe.exe	Suspicious	c:\users\sangfor\desktop\????\...	-	Observe	Pending	
□	11	lsass.exe.exe	Suspicious	c:\users\sangfor\desktop\????\...	-	Observe	Pending	
□	12	explorer.exe	Security issue	c:\windows\explorer.exe	2010-11-21 11:2...	-	Pending	

Page 1 of 1 | Entries Per Page: 50 | 1-17 of 1

Different Endpoints With The Same Malicious Domain Name/File Can Be Automatically Isolated & Blocked

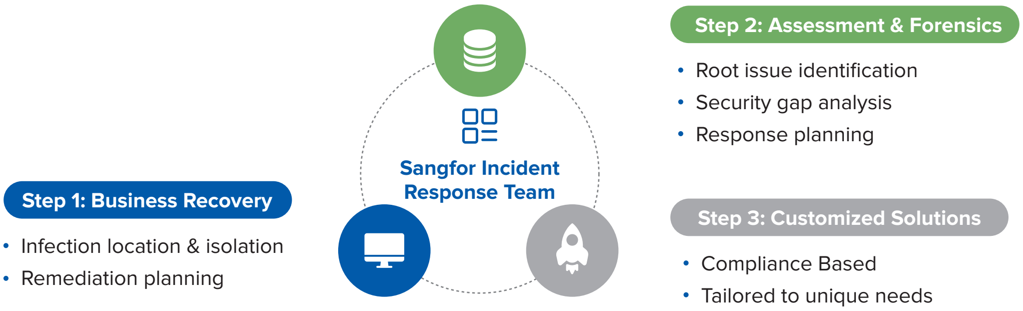


No.	Time	Host IP	Details	Type	Admin	Remark	Operati...
1	2019-10-18 16:22:08	192.168.11.10	Quarantine file (c:\windows\micr...	Quarantine File	admin	-	
2	2019-10-18 16:21:35	192.168.11.10	Quarantine file (c:\windows\micr...	Quarantine File	admin	-	
3	2019-10-08 19:05:49	192.168.11.10	Perform virus scan and removal...	Correlate to EDR	admin	-	-

Page 1 of 1 | Entries Per Page: 50 | 1-3 of 3

Sangfor Incident Response Services

04



Sangfor Incident Response Team

Step 1: Business Recovery

- Infection location & isolation
- Remediation planning

Step 2: Assessment & Forensics

- Root issue identification
- Security gap analysis
- Response planning

Step 3: Customized Solutions

- Compliance Based
- Tailored to unique needs

Sangfor Incident Response Services

05

Customer A: Government

Country	Ransomware	Response Timeline	Sangfor Solution
China	WannaCry	Recover Back-Up (1 hour) Virus Type Confirmation and Infected File Isolation (30 mins) ES Virus Removal (2 hours)	NGAF + Endpoint Secure + SIP

Customer B: Education

Country	Ransomware	Response Timeline	Sangfor Solution
Malaysia	GandGrab V2.1	Recover Back-Up (5 mins with Sangfor HCI) Virus Type Confirmation and Infected File Isolation (30 mins) ES Virus Removal (2 hours)	NGAF + Endpoint Secure

Customer C: Enterprise

Country	Ransomware	Response Timeline	Sangfor Solution
UAE	Phobos	Virus Type Confirmation and Infected File Isolation (30 mins) ES Virus Removal (2 hours) Vulnerability Scanning (2 hours)	NGAF + Endpoint Secure

For more information on the most powerful response to the threat of ransomware available, contact Sangfor Technologies at **www.sangfor.com** – and make ransomware protection and response simpler, more secure and more valuable.