Honda Cyber Attack: Analysis & Countermeasures

www.sangfor.com

SANGFOR

Background

In Dec 2019, a researcher found a publicly accessible unsecured Elasticsearch database cluster that exposed 26,000 North American Honda customer records. The database contained personally identifiable information (PII), vehicle information regarding make & model, vehicle identification numbers (VINs), and service information.

Source: Shutterstock

Disaster strikes again for the Japanese automobile manufacturer in June of 2020, when Honda's Twitter page posted the first in a series of messages warning customers of looming issues, saying that the customer service and financial departments were "experiencing technical difficulties and are unavailable."

Source: Twitter

The Culprit

SNAKE ransomware is strongly suspected to be the culprit of the Honda attack, with the SNAKE operators saying they would "not share details about the attack in order to allow the target some deniability." SNAKE is thought to be a relatively unsophisticated ransomware product, and is not thought to exfiltrate data, yet it is able to stop processes within the company network, with Industrial Control Systems (ICS) being a common target of the ransomware.

Analysis of the malware by Virtus Total shows that the internal domain mds.honda.com was found embedded in the SNAKE ransomware and used as a kill switch, because that domain is not resolvable from the internet. Ironically, SNAKE operators may have learned about that domain from another earlier Elasticsearch misconfiguration data breech in July 2019 that exposed 40GB of data including information about Honda's internal networks and systems.

The latest statement from Honda spokespeople to Forbes on June 10th says, "Honda has experienced a cyberattack that has affected production operations at some U.S. plants. However, there is no current evidence of loss of personally identifiable information. We have resumed production in most plants and are currently working toward the return to production of our auto and engine plants in Ohio." Plants in Ohio, Turkey, India, and Brazil remain suspended. A plant in the UK restored operations within a couple days.

While most assume that a company like Honda must have had the knowledge, skillset, funding, and sophistication to deploy a solid cyber security solution at their production sites, many secondary global sites operate with relative autonomy, in every industry. Let's take a look at a few of the solutions which might have been useful in protecting Honda in this situation.

The End of the Traditional Security Era

It is thought that the SNAKE Ransomware gained entry via a phishing attack, possibly **COVID-19 related**. Once a server was infected, the ransomware spread quickly and likely infecting production ICS servers, encrypting the data. Although Honda uses network firewalls and anti-virus products, SNAKE was smarter and able to circumvent both because there was little or no cooperation between the firewalls and the endpoint security technologies.

A more holistic solution would be where the firewall, when detecting Command & Control (C&C) communication, tells the endpoint security agent to rescan looking for infection. The rescan would have found the SNAKE files and would have prevented the ransomware from activating by telling the firewall to kill sessions to the C&C server, blocking download of command instructions.

A more robust endpoint security product would have the ability to detect the ransomware encryption process and immediately kill it while identifying and removing the controlling malware file. Then endpoint technology should then search all other systems looking for the same controlling file and removing it networkwide.

Technical Analysis of The Honda Incident

**All analysis is based on virus samples with assumptions made by Sangfor Security Team*

Step 1: The hacker group collected intranet information and Honda's IT system domain names, finally selecting the intranet address MDS.HONDA.COM as a backdoor. This intranet address is presumed to be Honda Group's internal IT service platform, and only internal employees can log in & use it.

Step 2: The hacker breached Honda's firewall system through RDP brute force or phishing emails (still unconfirmed), and then the hacker implanted a variant of the "Snake" ransomware, also known as "Ekans."

The hackers modified the virus feature to actively access the MDS.HONDA.COM intranet domain name through a zombie host. Once access has been gained, the zombie host will recognize it as an intranet host, and the virus will automatically encrypt the host. If the Zombie host is unable to access the intranet domain name MDS.HONDA.COM, then the host won't be recognized as an intranet host, and the Ransomware will remain dormant.

Step 3: Honda Group's endpoint anti-virus tools were bypassed allowing the "Ekans" ransomware to successfully encrypt the victims. The ransomware used a joint RSA+AES encryption algorithm, and currently, there are no global network security vendors that can decrypt it.

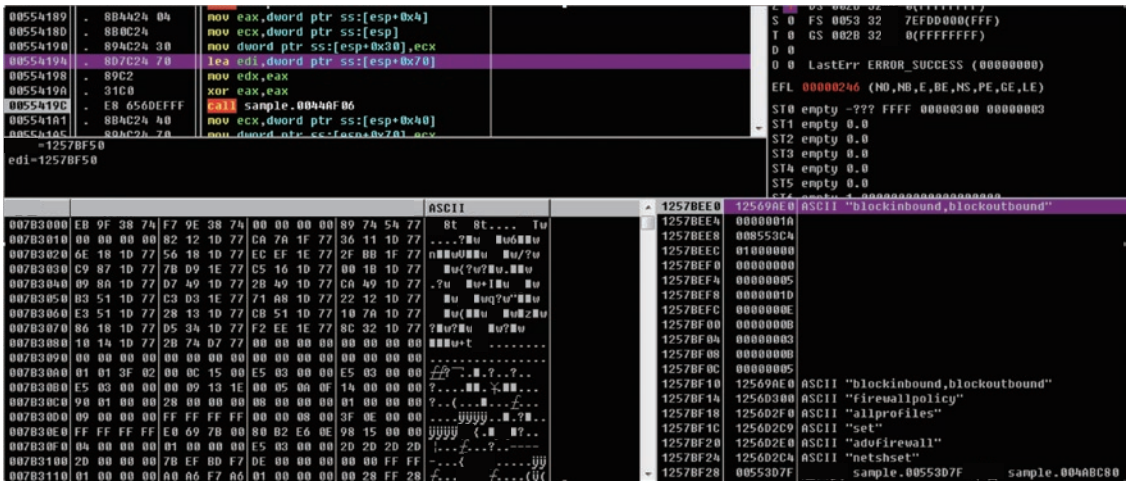
"Honda Ransomware Attack" Simulation & Sangfor Countermeasures

Step 1: Download the "Ekans" ransomware sample from VirusTotal (www.virustotal.com)

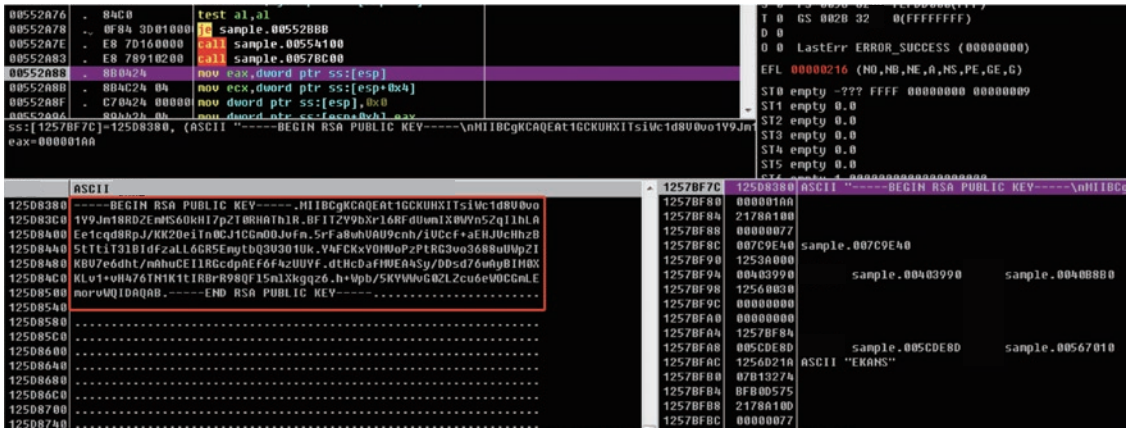
Step 2: Create a victim PC in a virtual machine environment, and then deploy Sangfor virtual Firewall and Endpoint Secure respectively.

Step 3: After closing the Sangfor Firewall and Endpoint Secure policies, the hacker is able to successfully implant EKANS ransomware to enter the victim's PC, and then initiate an execution command for the virus through C&C communication.

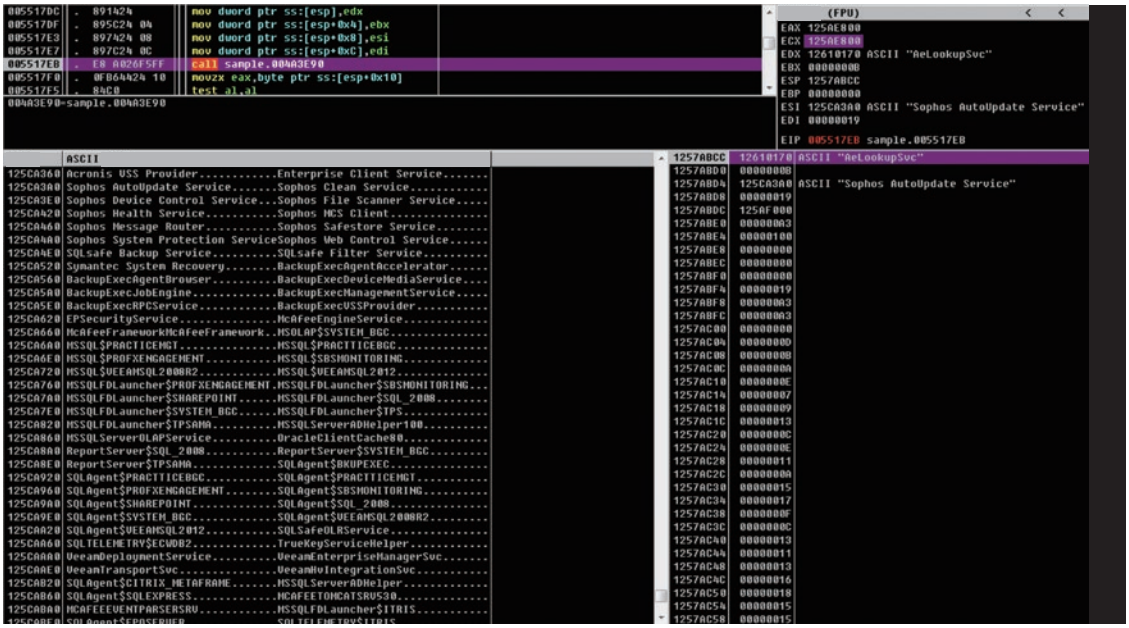
Step 4: The ransomware first modifies the inbound and outbound firewall configuration policies, preventing users from using remote control to end the encryption process, and then start instructing the victim host PC to actively access MDS.HONDA .COM.



Step 5: Assuming that the access was successful made, the “Ekans” ransomware starts to extract the RSA encrypted public key and starts the encryption process.



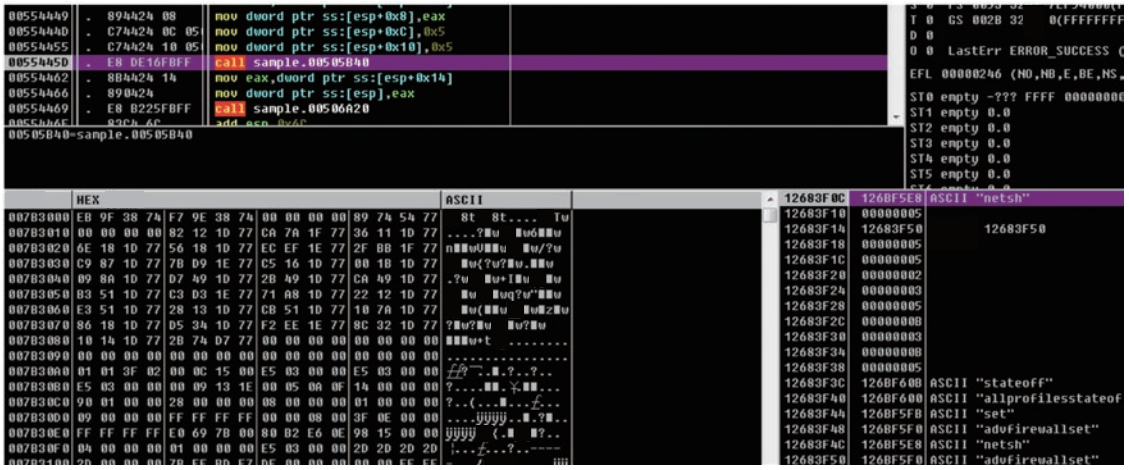
Step 6: The Ransomware will stop any anti-virus software, SQL and other services to ensure that the relevant files can be successfully encrypted.



Step 7: The encrypted file will save the original file name, encrypt it with AES key and other information, and add the "Ekans" wording at the end of the file name.

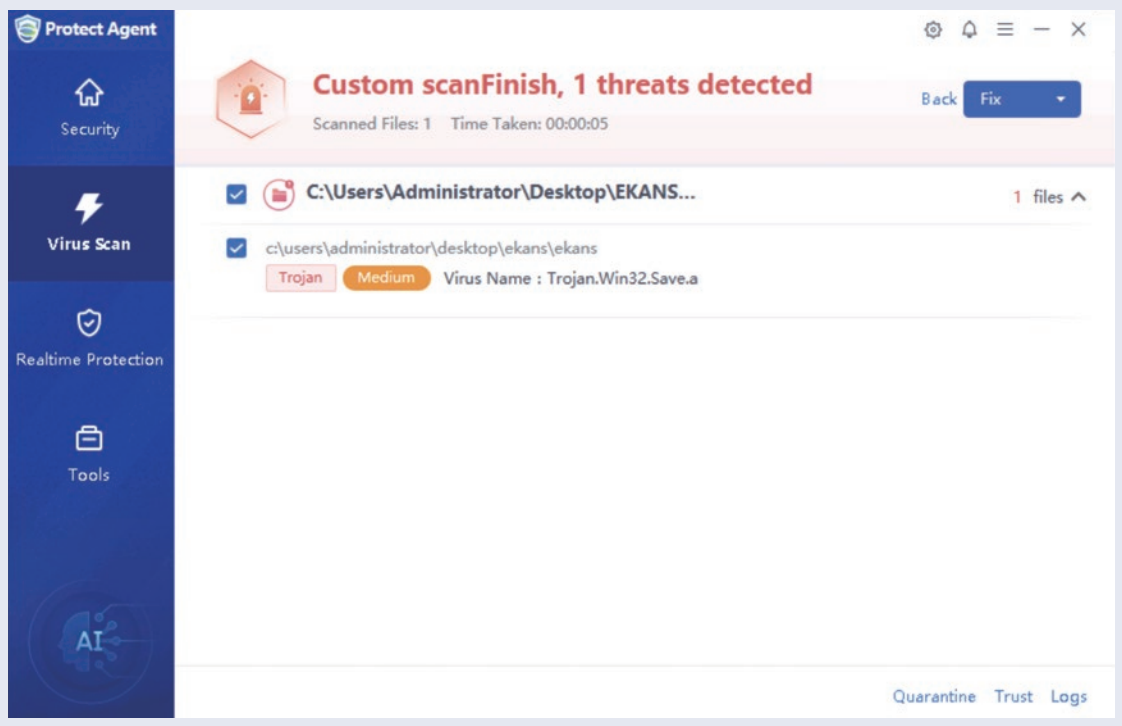
```
BC 5E D9 52 9B 2A 6C C1 29 B0 D6 33 63 D1 53 18   ¼^ÙR›*lÁ)°Ö3cÑS.
4A A2 30 74 9B 1A E6 20 89 58 36 00 4C FF 81 03   J¢0t›.æ ‰X6.Lÿ..
01 01 14 66 6A 6C 68 64 63 65 67 62 6D 69 64 70   ...fjlhdcegbmidp
6F 61 67 6C 6E 64 69 01 FF 82 00 01 03 01 08 46   oaglndi.ÿ,.....F
69 6C 65 4E 61 6D 65 01 0C 00 01 02 49 56 01 0A   ileName.....IV..
00 01 11 45 4E 43 52 59 50 54 45 44 5F 41 45 53   ...ENCRYPTED_AES
5F 4B 65 79 01 0A 00 00 00 FE 01 2A FF 82 01 0F   _Key.....þ.*ÿ,..
44 3A 5C 66 69 6C 65 5C 31 32 33 2E 74 78 74 01   D:\file\123.txt.
10 47 28 7A 18 90 48 AF 15 0C 57 98 D4 A0 A1 40   .G(z..H¯..W˜Ô ¡@
53 01 FE 01 00 91 1F 11 C3 79 52 FC A1 39 DE A1   S.þ..'..ÃyRü¡9Þ¡
9A 8A 08 07 C5 58 4E F2 C4 0B 64 89 21 6D 44 9E   šŠ..ÅXNòÄ.d‰!mDž
78 9E 20 B2 41 9C F6 4D 55 1B 43 4F C5 10 18 B0   xž ²AœöMU.COÅ..°
2C 87 29 19 89 E4 88 22 AE C0 39 E5 1C F7 A5 0C   ,‡).‰ä^"®À9å.÷¥.
D3 86 DE 36 C4 A9 A8 2E 46 BC AB 7A E6 19 C4 5C   Ó†Þ6Ä©¨.F¼«zæ.Ä\
28 E4 BF C5 B4 5B F8 92 BC D6 51 EA EA 47 D3 6E   (ä¿Å´[ø'¼ÖQêêGÓn
E9 81 06 31 B7 0F 46 3B 94 47 C1 15 9D 20 BE 08   é..1·.F;"GÁ.. ¾.
94 6F 21 11 0A 1D 55 D2 4C 89 59 D8 5E BD 02 C0   "o!...UÒL‰YØ^½.À
E4 30 92 20 60 6B 48 29 52 84 4F 4D 0D 81 A7 5F   ä0' `kH)R„OM..§_
93 00 E5 B8 1E 21 FA 5A B3 53 72 AC 69 F8 37 2A   ".å¸.!úZ³Sr¬iø7*
D1 B2 0A 7D B5 BC 88 2F 50 D9 60 F9 20 15 87 A1   Ñ².}µ¼ˆ/PÙ`ù .‡¡
26 B1 61 39 23 03 3D CB 86 03 35 73 90 6E 2C 75   &±a9#.=Ë†.5s.n,u
E2 77 09 ED 38 16 25 3B 1A 56 CE FF 34 AD 1A 05   âw.í8.%;.VÎÿ4-..
45 81 3B 34 3E 58 F8 28 44 84 F7 68 EE B0 BD D7   E.;4>Xø(D„÷hî°½×
0F 88 D9 F9 C8 E7 D6 F2 3B 45 8D C0 21 08 DB 96   .ˆÙùÈçÖò;E.À!.Û–
2C 6F DA 28 6D 00 D1 D6 4F 4F AC 28 5F 63 BD 49   ,oÚ(m.ÑÖOO¬(_c½I
E7 CB CC 2F E7 00 7A 01 00 00 45 4B 41 4E 53      çËÌ/ç.z...EKANS
```

Step 8: After the modification of the ransomware encryption is completed, the firewall policy that was modified before is restored to its original state, so that the victim can remotely connect to the firewall, and discover that he was hacked, through a series of security event notifications.



Step 9: Sangfor NGAF Firewall and Endpoint Secure provide a network/endpoint integration protection mechanism, removing the ransomware easily.

Sangfor NGAF Firewall can block the hacker's C&C communication, while Endpoint Secure isolates and kills the virus before it's activated.

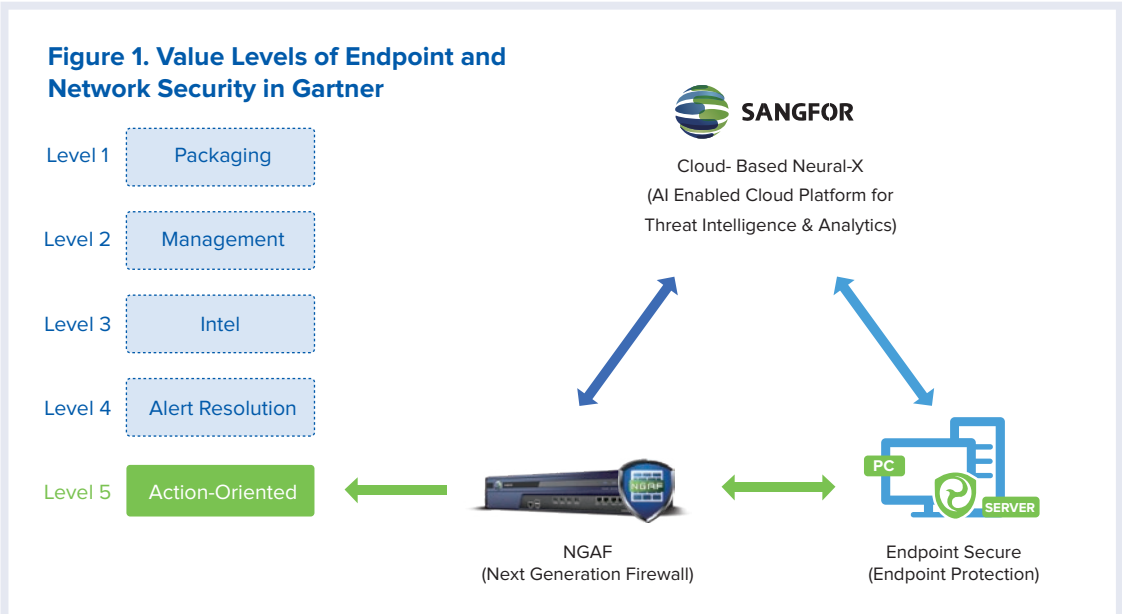


"Honda Ransomware Attack" Simulation & Sangfor Countermeasures

Sangfor provides a security solution, tailor made to protect against ransomware. This solution understands each step of the "kill chain" the malware uses to infiltrate, infect, and exploit a network and its systems. It is a holistic solution where solution components like the Sangfor Next-Generation Application Firewall (NGAF) integrates with, and communicates directly with the Sangfor Endpoint Secure agents to identify malicious network and endpoint behaviors and implement a coordinated response.

Endpoint Secure also has a built-in Ransomware Honeypot capable of detecting when ransomware starts to encrypt a file, stopping it, and then searching the organization for the same controlling file and deleting it from every system.
Gartner defines five levels of firewall and endpoint integration ability and Sangfor reaches the highest level of "Action-Oriented."

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



Watch a video of the Sangfor Security Solution for Ransomware in action here.
https://www.youtube.com/watch?v=YNUngrDG-Fg0&feature=youtu.be

Sangfor's Security Services for Ransomware

(1) Sangfor's Incident Response

In addition to its suite of advanced Security products, Sangfor also provides a closed-loop incident response service solution to organizations. 2020 has been a busy year, with Sangfor handling hundreds of manufacturing, finance & banking, education and ISP cases.

The scope of Sangfor's incident response service covers in-depth malware analysis and eradication, remediation and security incident reporting.

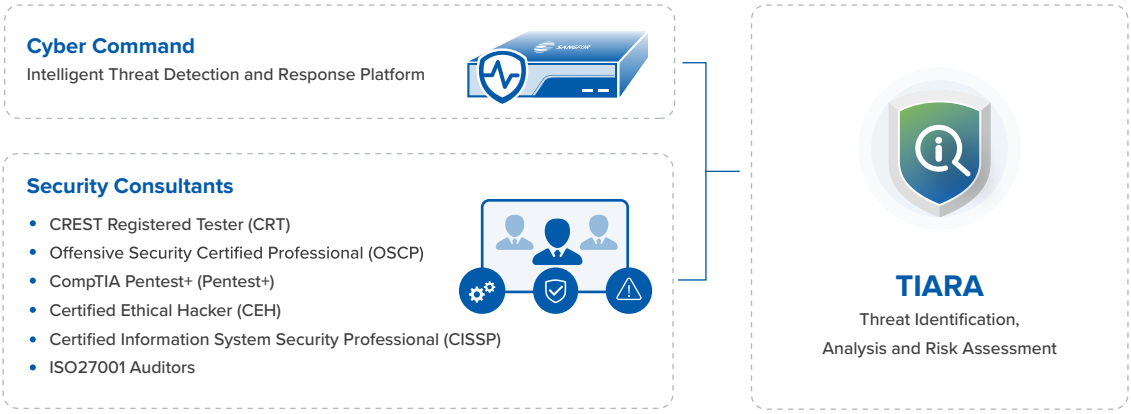
For more information about Sangfor Incident Response service, please visit our webpage.

(2) Sangfor's TIARA Service

TIARA is a turnkey service, including Sangfor HW, SW and Services, that helps customers quickly understand it current threat posture in just four weeks.

- Assessment: TIARA is a preliminary lightweight security posture assessment service which helps customers to determine the current threat posture of their complete network in a short period of time.

- Recommendation: TIARA also provides recommendations, improvement plans and remediation assistance to take overall security posture to the next level.



Why Sangfor?

Sangfor is committed to building the most useful, cutting-edge and next-level solutions for security, cloud and infrastructure. Sangfor updates are consistent, with our skilled R&D department constantly developing the most requested and needed malware, ransomware and malicious software protection solutions to our partners and customers.

Sangfor Technologies is an APAC-based, global leading vendor of IT infrastructure solutions specializing in Network Security and Cloud Computing. Visit us at www.sangfor.com to learn more about Sangfor's security solutions, and let Sangfor make your IT simpler, more secure and more valuable.