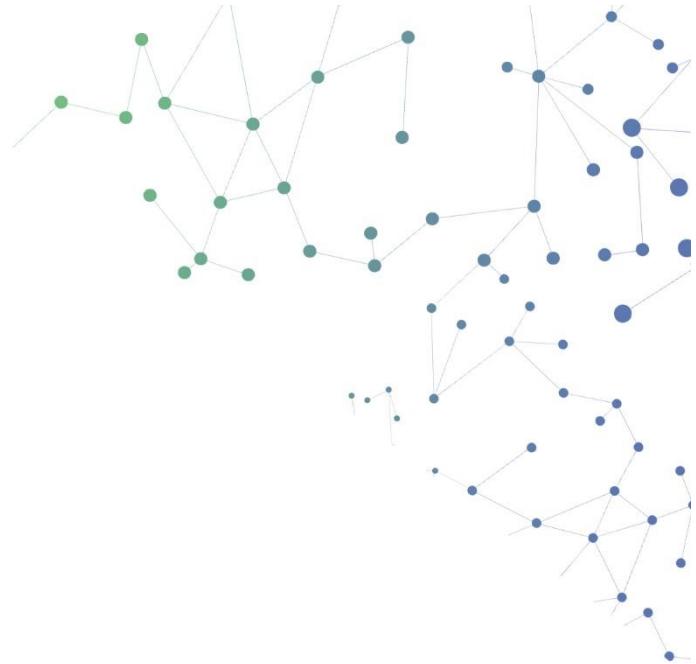


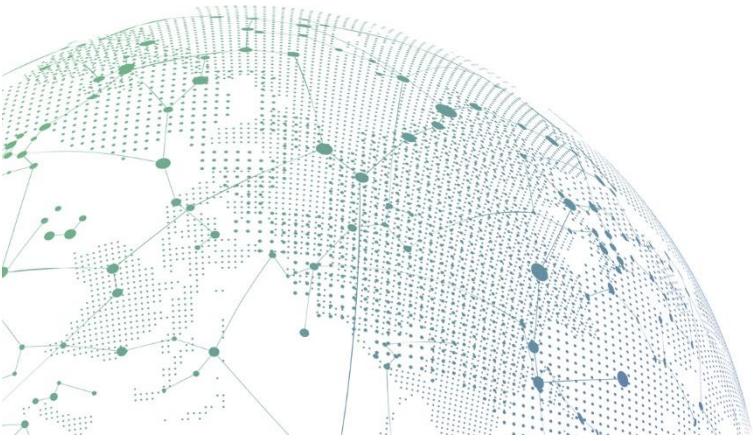


SANGFOR



Endpoint Secure

Praktik Terbaik untuk Skenario General Micro-Segmentation Policy



Catatan Perubahan

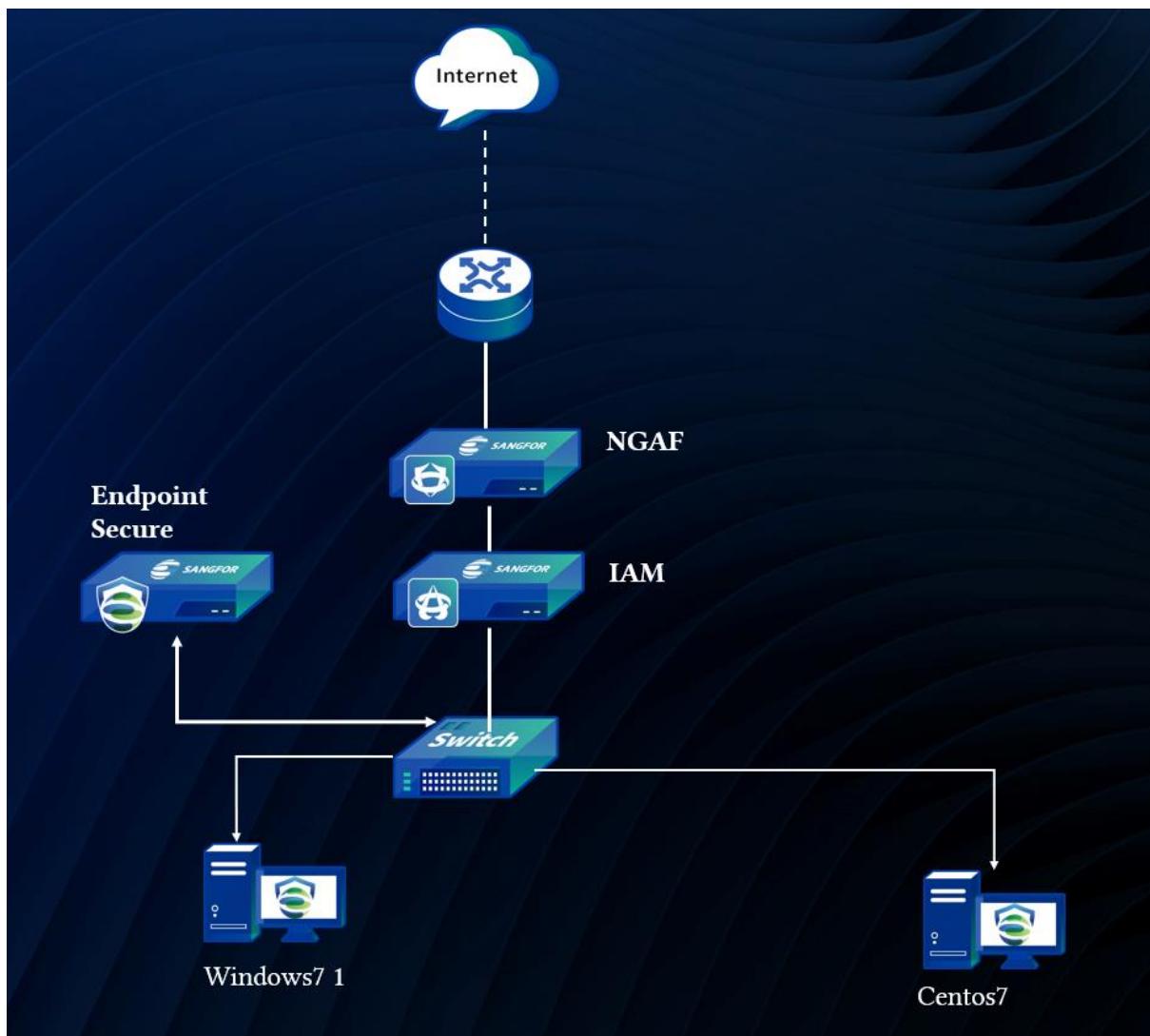
Tanggal	Deksripsi Perubahan
5 Janari 2020	Dokumen Terbit.
17 Mei 2021	Dokumen diperbarui.

CONTENT

Bab 1 Skenario	1
Bab 2 Latar Belakang.....	1
2.1 Konsep WFP	2
2.2 Untuk Endpoint Secure	2
Bab 3 Konfigurasi	2
3.1 Tentukan Policy Object	2
3.2 Tentukan Services	3
3.3 Buat Micro-Segmentation Policy.....	4
3.4 Periksa Policy Validity.....	5

Bab 1 Skenario

Dalam perusahaan ukuran kecil ataupun medium, ada zona DMZ di intranet untuk menyebarkan server untuk memberikan external web services, dan ada pengguna biasa mengakses internet di intranet. Sejak tidak adanya kebiasaan mengisolasi intranet, jadi pengguna intranet dapat mengakses server, ini dapat menempatkan server posisi beresiko, pada saat bersamaan, pengguna tidak dilarang untuk mengakses server. Karena itu diperlukan untuk melarang pengguna intranet mengakses port server yang beresiko tinggi untuk menghindari pengaksesan langsung pada port server yang beresiko tinggi oleh pengguna intranet.



Bab 2 Latar Belakang

2.1 Konsep WFP

Windows Filtering Platform (WFP) adalah basis framework untuk operasi interaktif pada paket data dalam lima layer dari stack protokol TCP/IP diluncurkan oleh windows.

Framework memberikan API seri untuk tujuan interaksi. Role dari framework ini adalah untuk mengganti teknologi TDI/NDIS/LSP sebelumnya.

Menggunakan WFP API, developer dapat menerapkan personal firewall, intrusion detection system, program antivirus, dan alat pemantau traffic. WFP terintegrasi fungsi kontrol process-based firewall, tetapi ini tidak firewall itu sendiri, ini hanya development framework untuk packet filtering.

2.2 Untuk Endpoint Secure

Micro-segmentation policy dapat menargetkan empat macam objek dari: Business Systems, Tags, Servers, IP Groups

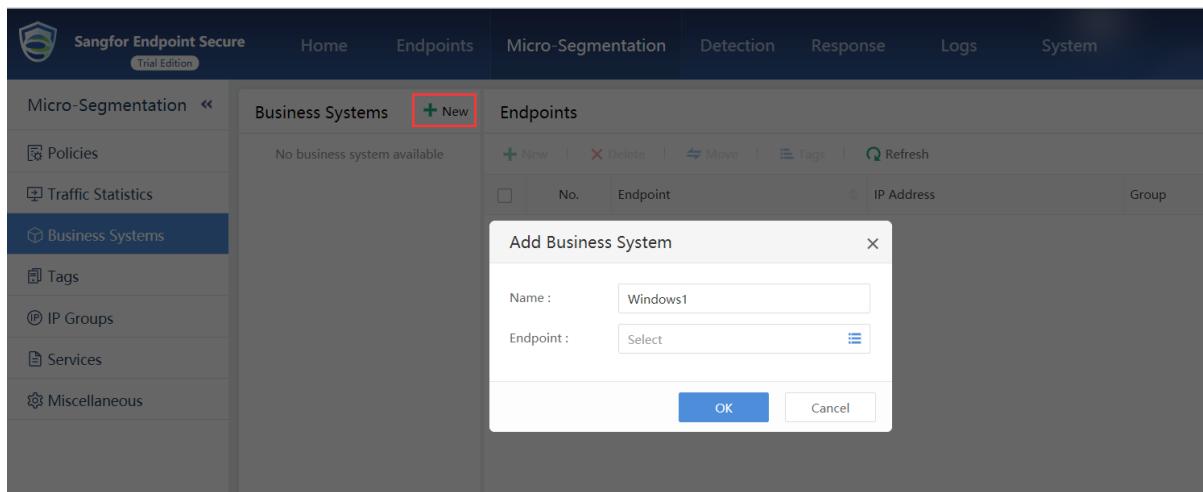
Kebutuhan Sistem Windows Vista, Windows 7, Windows 10

Windows Server 2008 dan versi selanjutnya.

Bab 3 Konfigurasi

3.1 Tentukan Policy Object

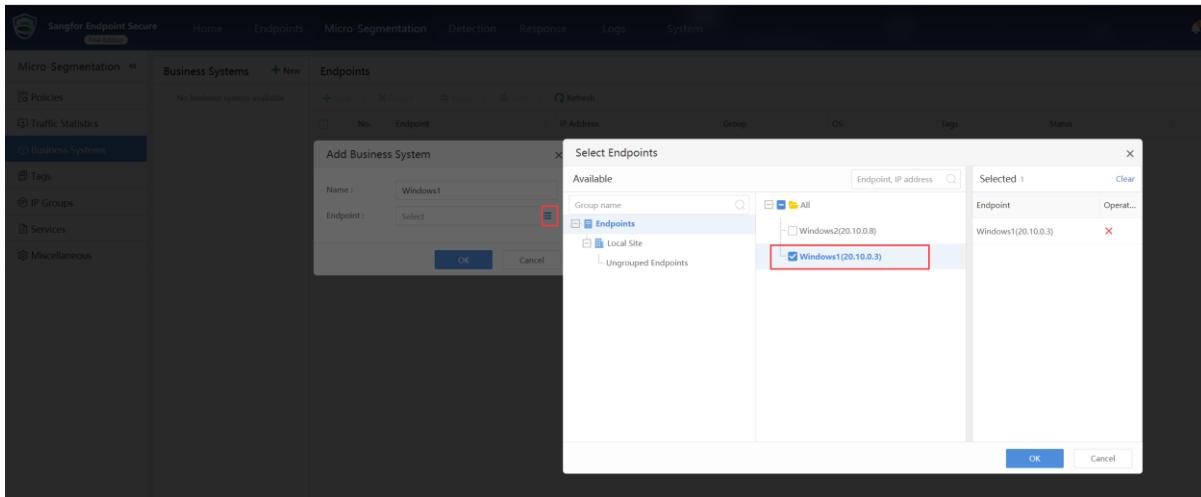
1.Tentukan Business System.



The screenshot shows the Sangfor Endpoint Secure interface. The top navigation bar includes Home, Endpoints, Micro-Segmentation, Detection, Response, Logs, and System. The left sidebar has tabs for Micro-Segmentation, Policies, Traffic Statistics, Business Systems (which is selected and highlighted in blue), Tags, IP Groups, Services, and Miscellaneous. The main content area shows a table for 'Business Systems' with a single row: 'No business system available'. Below this is a 'Endpoints' table with columns: No., Endpoint, IP Address, and Group. A modal window titled 'Add Business System' is displayed in the foreground, containing fields for 'Name:' (set to 'Windows1') and 'Endpoint:' (with a dropdown menu labeled 'Select'). At the bottom of the modal are 'OK' and 'Cancel' buttons.

2.Pilih spesifik endpoint.

General Micro-Segmentation Policy



3. Gunakan metode yang sama untuk menambahkan Business System Windows2 lainnya dan pilih spesifik endpoint.

The screenshot shows the Sangfor Endpoint Secure interface. The left sidebar has a 'Business Systems' section with a 'New' button highlighted by a red box. The main area shows a table for 'Endpoints'. A row for 'Windows1' is selected, indicated by a red box. The table columns are 'No.', 'Endpoint', and 'IP Address'. A single entry for 'Windows2' is listed with IP '20.10.0.8'.

3.2 Tentukan Services

1. Micro-Segmentation module mempunyai beberapa built-in services, tapi kalian dapat mengubah service secara manual. Seperti anti ransomware, kalian dapat membuat beberapa service yang mana termasuk port yang mana ransomware gunakan untuk brute force attack.

The screenshot shows the Sangfor Endpoint Secure interface. The left sidebar has a 'Services' section with a 'New' button highlighted by a red box. The main area shows a table for 'Services'. A row for 'Share' is selected, indicated by a red box. The table columns are 'No.', 'Name', 'Protocol', 'Port', 'Traffic Type', and 'Remarks'. Other services listed include Remote, Share, dhcp, mssql, ftp-data, ftp, ssh, telnet, smtp, and dns-t.

3.3 Buat Micro-Segmentation Policy

1.Klik Add untuk membuat Micro-segmentation policy, dan pilih Source/Destination Object.

The screenshot shows the Sangfor Endpoint Secure interface with the 'Micro-Segmentation' tab selected. On the left sidebar, 'Policies' is highlighted with a red box. In the main area, a 'New' button is also highlighted with a red box. A modal window titled 'Add New Policy' is open, containing fields for 'Policy Name' (set to 'Anti-Ransomware'), 'Source' (set to 'Windows1'), 'Destination' (set to 'Windows2'), and 'Action' (set to 'Deny'). The 'Services' field is set to 'Select'. The 'OK' button at the bottom of the modal is also highlighted with a red box.

2.Pilih services yang perlu untuk di blok, dan ubah Action as Deny.

This screenshot shows the same interface as the previous one, but the 'Services' field in the 'Add New Policy' modal is now populated with 'Remote(TCP,UDP:3389),Share(TCP,UDP:135,137,138,...)'. The 'Action' field is set to 'Deny', which is highlighted with a red box. The 'OK' button at the bottom of the modal is also highlighted with a red box.

3.Pastikan konfigurasi global dan konfigurasi policy enabled.

General Micro-Segmentation Policy

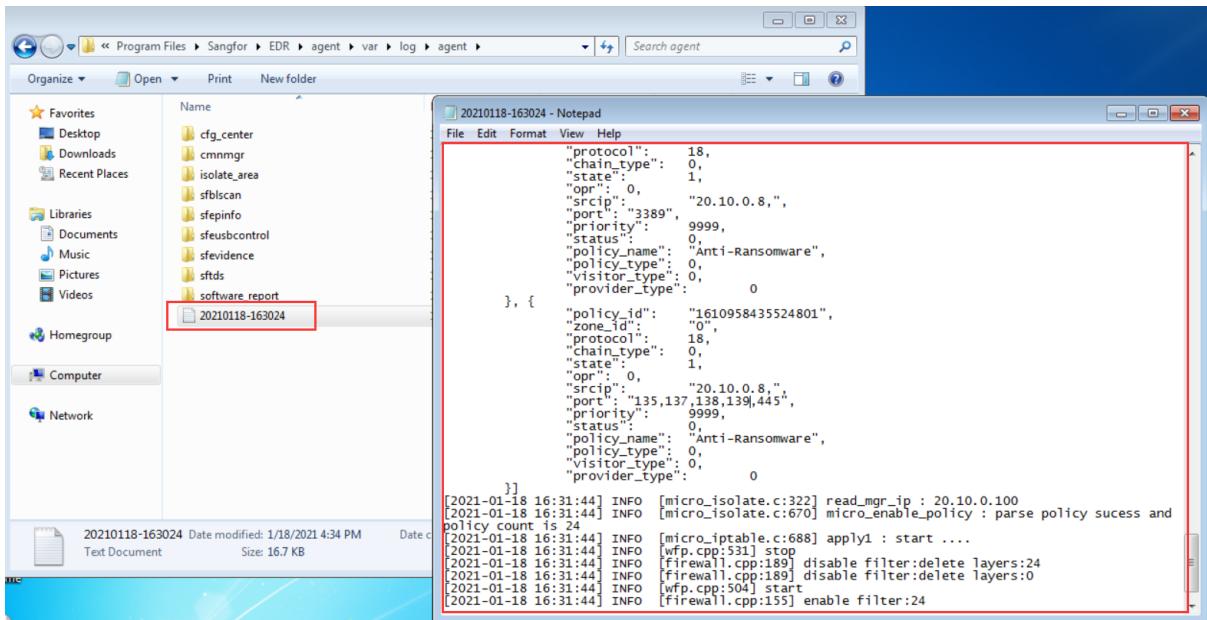
3.4 Periksa Policy Validity

1. Periksa agen log di endpoint.

Windows Agent log Path: **C:\Program Files\Sangfor\EDR\agent\var\log\agent**

Linux Agent log Path: **/sangfor/edr/agent/var/log/agent**

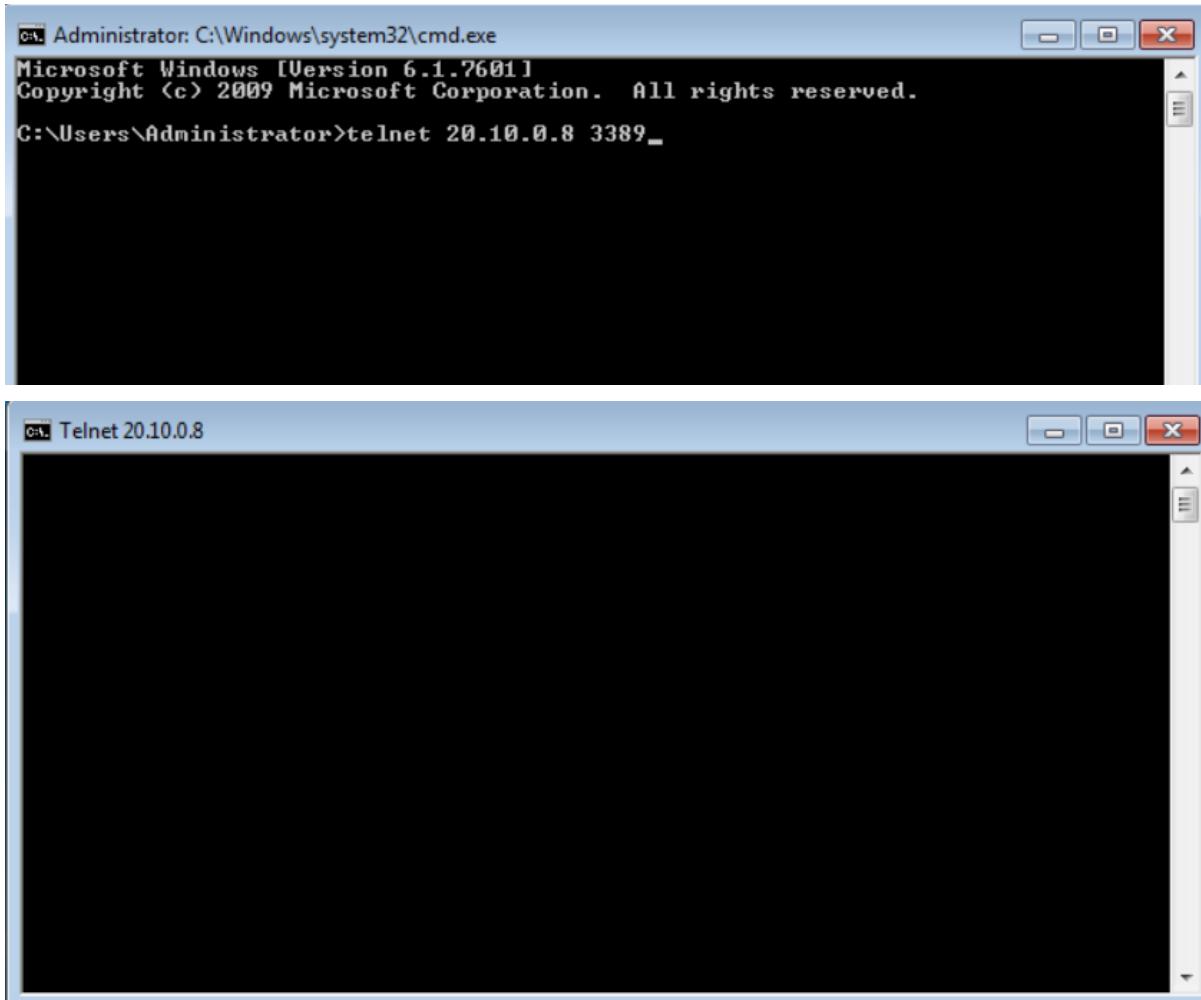
Jika kalian dapat melihat log sebagai berikut, berarti Micro-Segmentation policy telah berhasil.



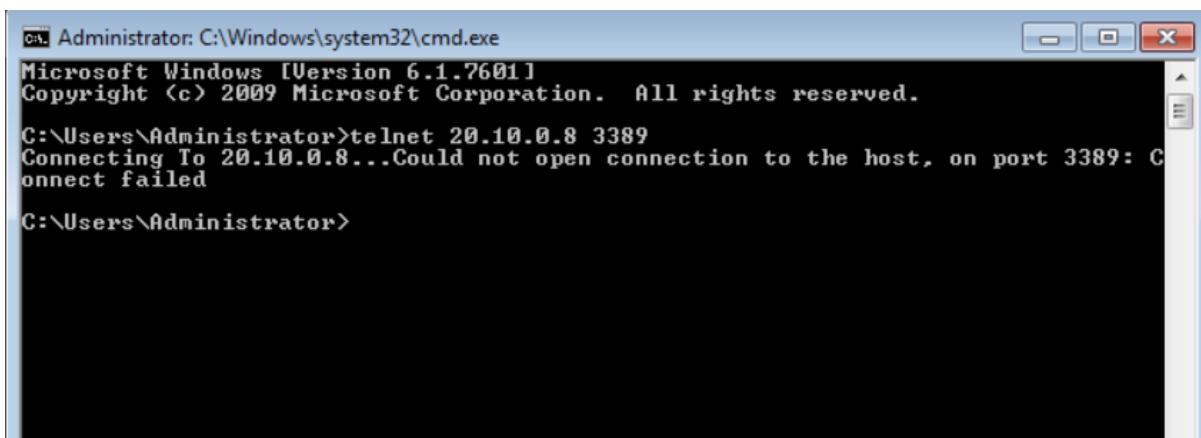
2. Gunakan telnet command untuk mengetes konektivitas port.

Sebelum mengaktifkan Micro-segmentation policy.

General Micro-Segmentation Policy



Setelah mengaktifkan Micro-Segmentation policy.





SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc