



#220151

November 2020

Commissioned by
Huawei Technologies Co., Ltd.

Huawei CloudEngine S6730-H Series 25GE Switches

Performance Evaluation and Feature Validation

Executive Summary

Huawei CloudEngine S6730-H series 25GE switches are full-featured fixed switches with 25GE downlink ports and 40GE/100GE uplink ports. They are ideal for enterprise campuses, higher education institutions, governments, data centers and telecommunication service providers.

Tolly engineers evaluated Huawei CloudEngine S6730-H series 25GE switches' performance and validated their features. Built upon Huawei's high performance Versatile Routing Platform (VRP) software, CloudEngine S6730-H series 25GE switches natively support WLAN Access Controller functionalities to manage up to 1,024 WLAN Access Points (APs) for convergence of wired and wireless networks. The CloudEngine S6730-H can be configured locally or work in cloud-managed mode to be managed by Huawei iMaster NCE-Campus (formerly Agile Controller). CloudEngine S6730-H series 25GE switches also support numerous security features and can interoperate with Huawei HiSec Insight Security Situation Awareness System (formerly CIS) for Encrypted Communications Analytics (ECA) and network-wide threat deception.

The Bottom Line

Huawei CloudEngine S6730-H Series 25GE Switches:

- 1 Support integrated wireless access controller functionality, allowing each switch to manage up to 1,024 WLAN APs
- 2 Support Huawei's Super Virtual Fabric (SVF) technology, which virtualizes core/aggregation devices (parent) and access devices (clients) into one logical device for easier management. SVF clients can include two layers of access switches (ASes) and one layer of WLAN APs, with ASes supporting stacked devices
- 3 Support VXLAN fabric with the BGP-EVPN control plane and distributed anycast gateways; support automated deployment of the VXLAN fabric using Huawei iMaster NCE-Campus

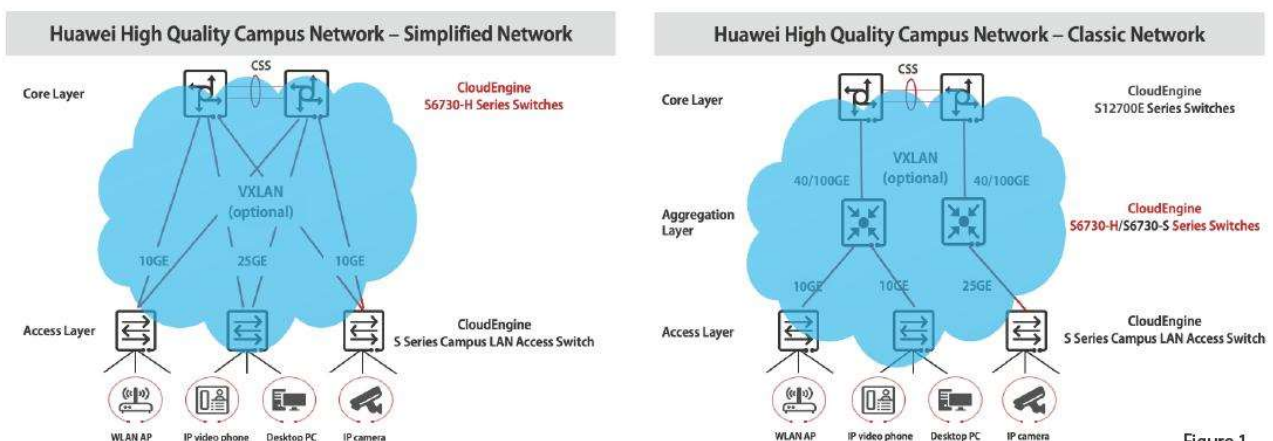


Figure 1



Test Results

Tolly engineers tested functions and performance of Huawei CloudEngine S6730-H series 25GE switches (hereinafter referred to as the S6730-H switch).

Test results apply to the Huawei CloudEngine S6730-H 25GE switch model CloudEngine S6730-H28Y4C. For summary of the test cases, refer to Table 2 and Table 3 on pages 7 and 8. Test results are as follows.

Port Capability

Port Performance

The 10GE SFP+ ports (25GE ports working in 10GE mode), 25GE SFP28 ports, 40GE QSFP+ ports (100GE ports working in 40GE mode), and 100GE QSFP28 ports on the S6730-H switch support line-rate forwarding of traffic with different frame sizes. See Table 1 for detailed results..

Device Capacity

MAC Table Capacity

The S6730-H switch supports 384K (393,216) MAC addresses in its MAC table. Tolly engineers verified that the switch forwarded traffic matching all entries in the MAC table, without frame loss or broadcasts occurring.

ARP Table Capacity

The S6730-H switch supports 140K entries in its ARP table. Tolly engineers verified that the switch forwarded traffic matching all entries in its ARP table, without any packet loss.

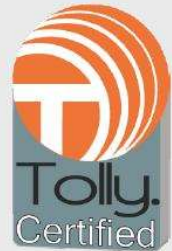
Routing Table/FIB Capacity

The S6730-H switch supports 256K (262,143) IPv4 routes in both its IPv4 routing table and FIBv4 table. Tolly engineers verified that the switch forwarded traffic matching all routing entries in the FIBv4 table, without any packet loss.

Huawei
Technologies Co.,
Ltd.

CloudEngine
S6730-H Series
25GE Switches

Performance
Evaluation and
Feature Validation



Tested
November
2020

The S6730-H switch supports 80K IPv6 routes in both its IPv6 routing table and FIBv6 table. Tolly engineers verified that the switch forwarded traffic matching all routing entries in the FIBv6 table, without any packet loss.

VLAN Capacity

The S6730-H switch supports 4K VLANs.

Huawei CloudEngine S6730-H Series 25GE Switch Performance (% of Line-rate)
(as reported by Spirent TestCenter)

Frame Size (Bytes)	64	128	256	512	1024	1280	1518
10GE Ports	100%	100%	100%	100%	100%	100%	100%
25GE Ports	100%	100%	100%	100%	100%	100%	100%
40GE Ports	100%	100%	100%	100%	100%	100%	100%
100GE Ports	100%	100%	100%	100%	100%	100%	100%

Notes: 100% line rate bidirectional traffic between two ports (same type) was used with zero frame loss. 10GE ports are 25GE ports working in 10GE mode. 40GE ports are 100GE ports working in 40GE mode.

Source: Tolly, November 2020

Table 1



ACL Capacity

The S6730-H switch supports 6K ACL rules. Tolly engineers verified that all ACL rules worked properly to match traffic and perform configured actions (e.g. deny).

NetStream Capacity

The S6730-H switch can monitor statistics of up to 1M flows (with different sources and destinations) using the NetStream feature.

Stack

Ports

Any ports on the S6730-H switch can be used for stacking.

Stack Bandwidth

The S6730-H switch supports 600Gbps unidirectional and 1.2Tbps bidirectional aggregated stack bandwidth. In the test, engineers used four 100GE ports and eight 25GE ports on the switch to stack with two other switches.

Loop-free/Ring Protocols

STP/RSTP/MSTP

The S6730-H switch supports the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).

ERPS

The S6730-H switch supports the Ethernet Ring Protection Switching (ERPS) protocol with less than 50ms failover time.

SEP

The S6730-H switch supports the Smart Ethernet Protection (SEP) protocol with less than 50ms failover time.

RRPP

The S6730-H switch supports the Rapid Ring Protection Protocol (RRPP) with less than 50ms failover time and less than 2.5ms fallback time.

Routing Protocols

The S6730-H switch supports IPv4 routing protocols such as RIP, OSPF, IS-IS, and BGP, as well as IPv6 routing protocols such as RIPng, OSPFv3, IS-IS for IPv6, and BGP4+.

VXLAN

Virtual Extensible LAN (VXLAN) is a major overlay network technology. VXLAN is used to build a Unified Virtual Fabric (UVF), which allows multiple service networks or tenant networks (virtual networks - VNs) to be deployed on the same physical network. The VNs are isolated from each other, implementing "one network for multiple purposes". This enables data transmission for different services or customers, while reducing network provisioning costs and improving network resource utilization.

Basic VXLAN Functions

The S6730-H switch supports the following basic VXLAN functions: virtual network (VN) creation, VN isolation, and Layer 2 (same bridge domain and network segment) and Layer 3 (different bridge domains and network segments) connectivity in the same VN.

BGP-EVPN Control Plane

The S6730-H switch uses BGP-EVPN as the control plane of the VXLAN overlay network and supports distributed anycast gateways.

Automated Configuration

Huawei iMaster NCE-Campus's Web GUI supports VXLAN-based fabric creation and configuration. Once the fabric creation is submitted, switch configurations are generated and deployed to S6730-H switches in an automated way.

VXLAN Resource Capacity

The S6730-H switch supports 16,000 IPv4 VXLAN tunnels or 4,000 IPv6 VXLAN tunnels. It supports 4,095 bridge domains in default mode or 16,000 bridge domains in super mode.

Cloud Management

The S6730-H switch support both local- and cloud-managed mode, ensuring smooth evolution and protecting customers' investments. In cloud-managed mode, the S6730-H switch is configured, monitored, and inspected on a cloud management platform, reducing onsite deployment and operations & maintenance (O&M) manpower, as well as network OPEX.

Tolly engineers verified that the S6730-H switch was able to be cloud-managed by Huawei iMaster NCE-Campus using the NETCONF protocol.



iPCA

Huawei's Packet Conservation Algorithm for Internet (iPCA) technology implements accurate packet loss monitoring and fast fault location on IP networks by coloring real service packets and monitoring packet quantities.

iPCA supports device-level, link-level and network-level packet loss measurement. Network-level packet loss measurement can be performed in an end-to-end, hop-by-hop, or regional manner.

Tolly engineers verified that the S6730-H switch supported all iPCA functions.

BFD

Bidirectional Forwarding Detection (BFD) can be used to quickly detect connectivity failures and trigger rapid traffic failover with technologies such as routing protocols.

3.3ms BFD Interval

The S6730-H switch can send BFD packets with 3.3ms intervals. The interval time is adjustable.

BFD for OSPF/BGP/VRRP

The S6730-H switch supports rapid OSPF/BGP route convergence and VRRP master node failover triggered by BFD forwarding path failure detection. The failover time of OSPF/BGP/VRRP with BFD was less than 50ms.

Security

Certain types of protocol packets including ARP requests, ICMP, DHCP Discover, etc. are sent to a switch's CPU for processing. It's critical that the switch provides certain attack defense features to prevent CPU overload.

CPU Attack Defense

Two functions of CPU Attack Defense were verified on the S6730-H switch by Tolly engineers.

Blacklist - Administrators can create a blacklist by defining an ACL. Then the switch discards any protocol packets matching the ACL rules.

CPCAR - Control Plane Committed Access Rate (CPCAR) limits the rate of protocol packets sent to the control plane. The switch can limit the traffic rate based on either the protocol type or ACL.

Attack Source Tracing

Three functions of Attack Source Tracing were verified on the S6730-H switch by Tolly engineers.

Whitelist - The switch does not trace the source of users in the whitelist, ensuring that valid protocol packets from users in the whitelist can be sent to the CPU for processing.

Attack source tracing - Administrators can set the threshold and sampling ratio for attack source tracing. When the number of protocol packets sent from an attack source in a specified period exceeds the threshold, the switch traces and logs the attack source to notify the administrator and perform attack source punishment.

Attack source punishment - Administrators can configure attack source punishment to discard or shut down the interface when an attack source is traced.

MFF

MAC-forced Forwarding (MFF) isolates user devices in a broadcast domain at Layer 2. MFF ensures that all traffic, including traffic in the same VLAN, is sent to the gateway, so

that the gateway can monitor data traffic and prevent malicious attacks between users. The S6730-H switch supports MFF.

IPSG

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP user-bind table (static or created by DHCP snooping).

After the IP or MAC address of a host was manually changed to not match the DHCP user-bind table, Tolly engineers verified that the host's IP traffic was all discarded by the S6730-H switch.

DAI

The S6730-H switch supports Dynamic ARP Inspection (DAI). ARP packets have to match the DHCP user-bind table (static or created by DHCP snooping) on IP, MAC, VLAN and interface to be forwarded.

DHCPv6 Snooping

The S6730-H switch supports the DHCPv6 snooping feature to make sure that only the DHCPv6 server connected to the trusted ports can distribute IPv6 addresses. It also creates the DHCP user-bind table to record the mapping of each client's IPv6 address, MAC addresses, VLAN and port.

ND Snooping

Neighbor Discovery (ND) snooping is a security feature of IPv6 ND and applies to Layer 2 networks. It creates the ND snooping user-bind table to record the mapping of source IPv6 addresses, MAC addresses, VLANs, and inbound ports of Neighbor Solicitation (NS) packets from IPv6 hosts. Tolly engineers verified that the S6730-H switch supported ND snooping.



SAVI

With the Source Address Validation Improvements (SAVI) feature, the S6730-H switch is able to check the validity of the source addresses in the Neighbor Discovery (ND) packets, DHCPv6 packets, and IPv6 data packets. The S6730-H switch is able to filter out invalid packets based on the user-bind table. The user-bind table is generated by ND snooping and DHCPv6 snooping. To check the validity of the source addresses in IPv6 data packets, the IP source guard feature needs to be enabled.

PPPoE+

PPPoE+, also called PPPoE Intermediate Agent is deployed on the switch that is located between the PPPoE client and the PPPoE server. It binds the user authentication information with the interface information to provide security for PPPoE access.

Tolly engineers verified that the S6730-H switch supported PPPoE+.

Secure Boot

Secure boot is the cornerstone of a secure system and secure storage. It ensures that the program to be run at each boot stage is a trusted one that has not been modified. Huawei uses the secure CPU, eFuse, and other security measures to ensure the boot security of the system. Starting from the hardware trust anchor, Huawei validates each step in the boot process. The system cannot boot if any boot step fails the validation process. Tolly engineers verified that a modified or forged digital signature image file cannot boot the system. The S6730-H switch reported a CRC error or signature error based on the modification type.

ECA

An increasing number of malware activities use encryption technologies to cover up malware transmission commands, control activities, or data breaches. Huawei's Encrypted Communication Analytics (ECA) technology extracts characteristics of encrypted traffic without decrypting the encrypted traffic, and reports the characteristics to Huawei HiSec Insight Security Situation Awareness System, a big data analytics system. Leveraging AI algorithms, Huawei HiSec Insight classifies and identifies normal and malicious encrypted traffic.

Tolly engineers verified that the S6730-H switch supported the ECA function.

Threat Deception

The S6730-H supports the threat deception function. With this function enabled, a switch functions as a sensor, detects threats such as IP address scanning on a network, and diverts the threat traffic to the honeypot for further checks. The honeypot performs in-depth interaction with the initiator of the threat traffic, records various application-layer attack methods of the initiator, and reports security logs to Huawei HiSec Insight for analysis. If Huawei HiSec Insight determines that the suspicious traffic is an attack, it generates an alarm and provides handling suggestions. After an administrator acknowledges the alarm, Huawei HiSec Insight delivers a policy to the switch through Huawei iMaster NCE-Campus to process the security event, ensuring security of the campus network.

Tolly engineers verified the following types of proactive defense using threat deception technology:

- When an attacker pinged a nonexistent IP address (one not used by any device), the S6730-H switch

redirected the ping request to Huawei HiSec Insight. Huawei HiSec Insight responded to the ping request by simulating the endpoint and recorded the attack event.

- When an attacker attempted to access an HTTP page with a nonexistent IP address, the S6730-H switch redirected the access request to Huawei HiSec Insight. Huawei HiSec Insight responded to the request by simulating the corresponding web server and recorded the attack event.

Authentication

802.1X/MAC/Web Portal Authentication

The S6730-H switch can work as the authentication policy enforcement point to implement 802.1X authentication, MAC authentication, and web portal authentication for users. The S6730-H switch can support up to 10,000 concurrent online users.

Free Mobility

The S6730-H switch supports free mobility based on user control list (UCL) groups. With a UCL group, an administrator can create an ACL rule, "rule 1 deny IP source UCL-group name Test destination [File Server's IP address]", to dynamically prevent users in the "Test" UCL group from accessing the file server. Each user is granted the same network access permission regardless of whether the user is a wired or wireless user, where the user logs in, and which IP address the user obtains.



Device Management

Zero Touch Provisioning (ZTP)

The S6730-H switch can work with Huawei eSight Unified Management System, to implement zero touch provisioning (ZTP).

The out-of-box S6730-H switch also supports plug-and-play with Huawei iMaster NCE-Campus.

Super Virtual Fabric (SVF)

On a traditional campus network, a large number of access devices are widely distributed and have similar configurations. If these devices are configured and managed via traditional methods, a large amount of work is repeated. Huawei's SVF technology virtualizes core/aggregation devices and access devices (including access switches for wired access and WLAN APs for wireless access) into one logical device. The SVF parent (core/aggregation device) manages and configures SVF clients (access devices), simplifying network management and configuration.

An SVF system's clients support two layers of Access Switches (ASes) and one layer of

WLAN APs, with ASes supporting stacked devices.

Tolly engineers verified that the S6730-H switch was able to function as a parent or AS in an SVF system.

Intelligent Upgrade

The S6730-H switch can be connected to Huawei Online Upgrade Platform (HOUP) to implement intelligent upgrade.

WLAN

The S6730-H switch supports integrated wireless access controller functionality to manage up to 1,024 WLAN APs.

Test Methodology

Capacity

In the capacity test, each item was tested independently.

Huawei CloudEngine S6730-H Series 25GE Switches



CloudEngine S6730-H28Y4C

Source: Tolly, November 2020

Figure 2



Huawei CloudEngine S6730-H Series 25GE Switches Tolly Verified Features - Part 1 of 2

Interface Capability		Loop-free/Ring Protocol	
✓	10GE Ports Port-to-port Line-rate Forwarding (64- to 1518-Byte RFC2544 standard frame sizes)	✓	STP/RSTP/MSTP
✓	25GE Ports Port-to-port Line-rate Forwarding (64- to 1518-Byte RFC2544 standard frame sizes)	✓	Ethernet Ring Protection Switching (ERPS) with less than 50ms failover convergence time
✓	40GE Ports Port-to-port Line-rate Forwarding (64- to 1518-Byte RFC2544 standard frame sizes)	✓	Smart Ethernet Protection (SEP) with less than 50ms failover convergence time
✓	100GE Ports Port-to-port Line-rate Forwarding (64- to 1518-Byte RFC2544 standard frame sizes)	✓	Rapid Ring Protection Protocol (RRPP) with less than 50ms failover convergence time and 2.5ms fallback convergence time
Device Capacity		VXLAN	
✓	MAC table: 384K MAC addresses	✓	Basic VXLAN functions: Virtual Network (VN) isolation, Layer 2 and Layer 3 connectivity in a VN
✓	ARP table: 140K entries	✓	BGP EVPN control plane and distributed anycast gateways
✓	Routing table: 256K IPv4 routes 80K IPv6 routes	✓	VXLAN configuration automation using Huawei iMaster NCE-Campus
✓	FIB: 256K IPv4 forwarding entries 80K IPv6 forwarding entries	✓	Bridge Domain Capacity: Default mode - 4,095 BDs Super mode - 16,000 BDs
✓	VLAN: 4K VLANs	✓	VXLAN Tunnels: 16,000 IPv4 tunnels 4,000 IPv6 tunnels
✓	ACL: 6K ACL rules	Cloud-managed Mode	
✓	NetStream: Monitoring 1M traffic flows	✓	Managed by cloud management platforms (e.g. Huawei iMaster NCE-Campus in public or private cloud) via NETCONF
Stack		iPCA	
✓	Stack with any ports on the switch	✓	Huawei Packet Conservation Algorithm for Internet (iPCA) Device-level, link-level and network-level packet loss monitoring without traffic overhead
✓	Stack Bandwidth: 600Gbps each direction, 1.2Tbps bidirectional aggregated	BFD	
Routing Protocol		✓	Sending BFD packets with 3.3ms intervals
✓	RIP / OSPF / IS-IS / BGP	✓	BFD for OSPF, BFD for BGP, BFD for VRRP less than 50ms failover time
✓	RIPng / OSPFv3 / IS-IS for IPv6 / BGP4+		

Source: Tolly, November 2020

Table 2



Huawei CloudEngine S6730-H Series 10GE Switches Tolly Verified Features - Part 2 of 2

Security		Authentication (as the Network Access Control - NAC Policy Enforcement Point)	
✓	CPU defend policy - CPCAR Device level rate limit for traffic of certain protocols (e.g. ICMP, ARP, etc.) to protect the CPU	✓	802.1X authentication
✓	CPU defend policy - blacklist Device level blacklist to block known attackers	✓	MAC authentication
✓	Attack source tracing Interface level feature. Identify the attacker and respond with certain actions (interface error down, alarm, etc.)	✓	Web authentication (portal authentication)
✓	MAC-Forced Forwarding (MFF) Layer 2 isolation. All Layer 2 communications have to go through the gateway	✓	10,000 concurrent authenticated users
✓	Dynamic ARP Inspection (DAI) Prevent man-in-the-middle attacks and theft on authorized users' information. The device validates ARP packets' source IP, source MAC, VLAN ID and interface with the binding table (static or DHCP snooping)	✓	Free Mobility with consistent user access experience regardless of the user location
✓	IP Source Guard (IPSG) Prevent IP address spoofing attacks (unauthorized hosts access and attack the network with forged IP addresses). The device validates IP packets' source IP, source MAC, VLAN ID and interface with the binding table (static or DHCP snooping)	Device Management	
✓	DHCPv6 snooping Trusted port for the DHCPv6 server; Binding table creation	✓	Zero Touch Provisioning (ZTP) with Huawei eSight Unified Management System
✓	ND snooping Trusted port for ND; Binding table creation	✓	Plug-and-play with Huawei iMaster NCE-Campus
✓	Source Address Validation Improvements (SAVI) Validate DHCPv6, ND and IPv6 packets with the binding table	✓	Super Virtual Fabric (SVF) Parent node or Access Switch (AS) role
✓	PPPoE+ (PPPoE Intermediate Agent) Add the PPPoE client-side interface information to the PPPoE packets for the BRAS to distinguish between end hosts	✓	Intelligent upgrade with the Huawei Online Upgrade Platform (HOUP)
✓	Secure boot CRC check, signature check and other methods to ensure the switch boots from a legit image	WLAN	
✓	Encrypted Communication Analysis (ECA) Report the attack to Huawei HiSec Insight. Perform the action assigned in Huawei HiSec Insight (via Huawei iMaster NCE-Campus in the middle)	✓	Native wireless access controller functionality to manage up to 1,024 Huawei WLAN Access Points (APs)
✓	Threat deception Route ping sweep and other IP/port scanning traffic to Huawei HiSec Insight. Perform the action assigned in Huawei HiSec Insight (via Huawei iMaster NCE-Campus in the middle)		
✓	MACsec		

Source: Tolly, November 2020

Table 3





About Tolly

The Tolly Group companies have been delivering world-class ICT services for 30 years. Tolly is a leading global provider of third-party validation services for vendors of ICT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
<http://www.tolly.com>

Test Equipment Summary

Vendor	Product	Web
Huawei	CloudEngine S6730-H28Y4C VRP software, Version 5.170 (S6730V200R020C00SPC200)	 HUAWEI https://e.huawei.com
Spirent	TestCenter	 spirent™ <small>Promise. Assured.</small> https://www.spirent.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

220151 ivcofs46 yx-20201125-VerL