Tolly TEST REPORT

#225147

August 2025

Commissioned by
Arctic Wolf Networks, Inc.

Aurora Endpoint Security

Efficacy with Endpoint Detection & Response

EXECUTIVE SUMMARY

Traditionally, endpoint security solutions impose performance overhead on enterprise systems. This resource consumption directly impacts user productivity, application response times, and total cost of ownership. Organizations require data on both protection efficacy and system resource utilization to make informed security architecture decisions. This evaluation examines Arctic Wolf's Aurora Endpoint Security across both dimensions.

Arctic Wolf commissioned Tolly to benchmark the threat protection efficacy, system resource consumption, and endpoint detection & response features of its Aurora Endpoint Security solution in a Windows 11 environment.

Results demonstrate Aurora Endpoint Security achieved 100% malware protection rates while consuming approximately 33% CPU resources during scanning operations. Aurora Endpoint Defense (NGAV + EDR) successfully intercepted all stages of a multi-phase cyberattack simulation. These characteristics address requirements for resource-constrained and operational technology environments with limited computing capacity.

See Figure 1 for a summary of endpoint protection results.

THE BOTTOM LINE

Aurora Endpoint Security:

1. Delivered robust security with 100% threat prevention, ensuring safety from diverse & evolving threats
2. Achieved low and steady CPU consumption while scanning, enabling uninterrupted user productivity and extending endpoint hardware lifecycles
3. Provided advanced behavioral EDR capabilities, detecting and stopping multi-stage attacks that signature-based solutions miss

Windows 11 Endpoint Protection Efficacy & Resource Utilization
Scanning A Collection of 1,000 Recent Virus Samples
(Detection % determined by number of files remaining in folder after scan)

	Illustrative Industry Composite[1]	ARCTIC WOLF
Efficacy	~85 - 95%	100% ✓
Avg. CPU	~60%+	~33% ✓

Aurora Endpoint Security has **Higher Efficacy** with **Lower Resource Utilization** than Alternative Industry Solutions

[1] Illustrative though informed from prior testing. Note: Scan is triggered by system decompressing a password-protected "zip" file containing 1,000 malware samples sourced from a major public source. Same sample set used for each solution. Higher efficacy and lower CPU utilization are the better results. CPU utilization was averaged across the duration of the scan.

Source: Tolly, August 2025

Figure 1

Report link: https://www.tolly.com/publications/225147

Test Results

Background

Endpoint protection solutions, by their very nature, are always present and, thus, always consuming at least some system resources. If an endpoint security solution consumes excessive resources, such as CPU, then response time for the end user and business applications may suffer.

The nature of this test is very focused, and the results can be presented quite succinctly. To benchmark the resource consumption and efficacy of Aurora Endpoint Security, Tolly evaluated both the threat protection effectiveness and the resource consumption when scanning folders containing 1,000 recent malware samples. The endpoint had access to the Internet, and was able to query their centralized databases when examining the malware, in addition to its local information. The key test results are summarized in Figure 1 on the previous page. A visual representation of the solution in-use can be found in Figure 2. Details of specific policy settings tested are found in Table 1 near the end of the report.

Efficacy

Aurora Endpoint Security demonstrated exceptional threat detection capabilities, successfully identifying and quarantining 100% of the 1,000 malware samples. This protection rate represents a comprehensive validation of the solution's ability to identify diverse malware variants in real-world conditions.

Resource Utilization

As noted, a particular focus of this test was how the endpoint solution managed precious Windows resources. Given that endpoint solutions typically are at work in the background and the arrival of malware is unpredictable, it can be very challenging to pinpoint resource usage.

For that reason, Tolly used folders containing 1,000 samples to drive the test. The results showed that Arctic Wolf's use of CPU resources during the test was very minimal. Total CPU utilization was approximately 33% for the test, enabling users to maintain productivity while staying protected. See Figure 2.

While the scenario tested is not being put forth as a common scenario, it does illustrate that Aurora Endpoint Security performs effectively while limiting their usage of CPU resources. This advantage allows for consistent performance for end users going about their business tasks, without being hamstrung by an overly resource-intensive program.

Arctic Wolf Networks, Inc.

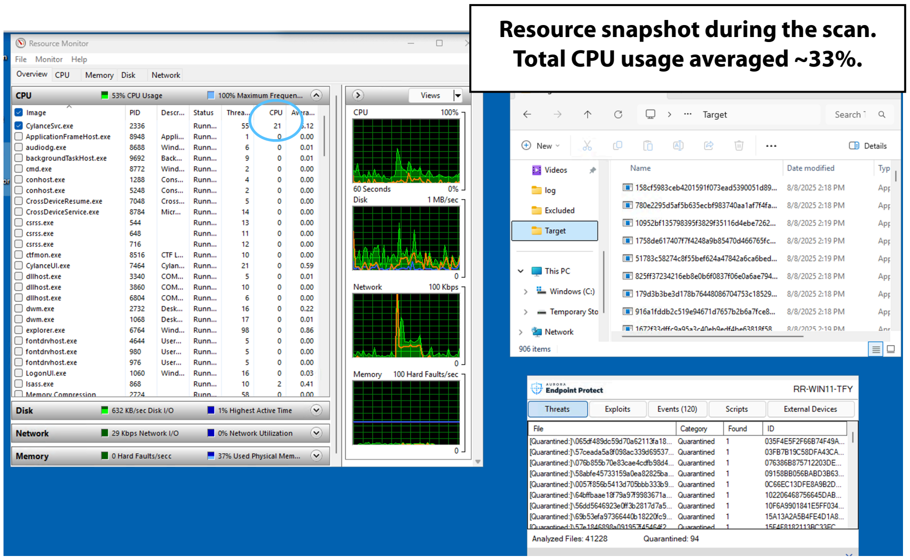
Aurora Endpoint Security

Efficacy & Endpoint Detection Response

Tolly Certified

Tested August 2025

Aurora Endpoint Security
Windows 11 Resource Utilization During Scan
(as reported by Microsoft Resource Monitor)



Resource snapshot during the scan.
Total CPU usage averaged ~33%.

Resource Monitor

CPU — 53% CPU Usage — 100% Maximum Frequen...

☑ Image	PID	Descr...	Status	Threa...	CPU	Avera...
☑ CylanceSvc.exe	2336		Runn...	55	21	6.12
☐ ApplicationFrameHost.exe	8948	Appli...	Runn...	1	0	0.00
☐ audiodg.exe	8688	Wind...	Runn...	6	0	0.01
☐ backgroundTaskHost.exe	9692	Back...	Runn...	9	0	0.01
☐ cmd.exe	8772	Wind...	Runn...	2	0	0.00
☐ conhost.exe	1288	Cons...	Runn...	4	0	0.00
☐ conhost.exe	5248	Cons...	Runn...	2	0	0.00
☐ CrossDeviceResume.exe	7048	Cross...	Runn...	5	0	0.00
☐ CrossDeviceService.exe	8784	Micr...	Runn...	14	0	0.00
☐ csrss.exe	544		Runn...	13	0	0.00
☐ csrss.exe	648		Runn...	11	0	0.00
☐ csrss.exe	716		Runn...	12	0	0.00
☐ ctfmon.exe	8516	CTF L...	Runn...	10	0	0.00
☐ CylanceUI.exe	7464	Cylan...	Runn...	21	0	0.59
☐ dllhost.exe	3340	COM...	Runn...	5	0	0.01
☐ dllhost.exe	3860	COM...	Runn...	10	0	0.00
☐ dllhost.exe	6804	COM...	Runn...	6	0	0.00
☐ dwm.exe	2732	Desk...	Runn...	16	0	0.22
☐ dwm.exe	1068	Desk...	Runn...	17	0	0.01
☐ explorer.exe	6764	Wind...	Runn...	98	0	0.86
☐ fontdrvhost.exe	4644	User...	Runn...	5	0	0.00
☐ fontdrvhost.exe	980	User...	Runn...	5	0	0.00
☐ fontdrvhost.exe	976	User...	Runn...	5	0	0.00
☐ LogonUI.exe	1060	Wind...	Runn...	16	0	0.03
☐ lsass.exe	868		Runn...	10	2	0.41
☐ Memory Compression	2724		Runn...	58	0	0.00

Disk — 632 KB/sec Disk I/O — 1% Highest Active Time

Network — 29 Kbps Network I/O — 0% Network Utilization

Memory — 0 Hard Faults/secc — 37% Used Physical Mem...

Name	Date modified	Typ
158cf5983ceb4201591f073ead5390051d89...	8/8/2025 2:18 PM	App
780e2295d5af5b635ecbf983740aa1af7f4fa...	8/8/2025 2:18 PM	App
10952bf135798395f3829f35116d4ebe7262...	8/8/2025 2:19 PM	App
1758de617407f7f4248a9b85470d466765fc...	8/8/2025 2:19 PM	App
51783c58274c8f55bef624a47842a6ca6bed...	8/8/2025 2:19 PM	App
825ff37234216eb8e0b6f0837f06e0a6ae794...	8/8/2025 2:18 PM	App
179d3b3be3d178b76448086704753c18529...	8/8/2025 2:18 PM	App
916a1fddb2c519e94671d7657b2b6a7fce8...	8/8/2025 2:18 PM	App
1672f33dffc9a95a3c40eb9edf4be63818f58	8/8/2025 2:19 PM	App

906 items

AURORA Endpoint Protect — RR-WIN11-TFY

File	Category	Found	ID
[Quarantined:]\065df489dc59d70a62113fa18...	Quarantined	1	035F4E5F2F66B74F49A...
[Quarantined:]\57ceada5a8f098ac339d69537...	Quarantined	1	03FB7B19C58DFA43CA...
[Quarantined:]\076b855b70e83cae4cdfb98d4...	Quarantined	1	076386B875712203DE...
[Quarantined:]\58abfe45733159a0ea82825ba...	Quarantined	1	09158BB056BABD3B63...
[Quarantined:]\0057f856b5413d705bbb333b9...	Quarantined	1	0C66EC13DFE8A9B2D...
[Quarantined:]\64bffbaae18f79a97f9983671a...	Quarantined	1	10220646875664 5DAB...
[Quarantined:]\56dd5646923e0ff3b2817d7a5...	Quarantined	1	10F6A9901841E5FF034...
[Quarantined:]\69b53efa97366440b18220fc9...	Quarantined	1	15A13A2A5B4FE4D1A8...
[Quarantined:]\57e1846898a091957f45464f2	Quarantined	1	15F4E8182113BC33FC

Analyzed Files: 41228 Quarantined: 94

Source: Tolly, August 2025

Figure 2

How Aurora Focus Protects Against Real World Threats

EDR Overview

Endpoint Detection and Response (EDR) monitors endpoint behavior in real-time, identifying suspicious activities through behavioral analysis rather than signature-based detection. Arctic Wolf's EDR solution, Aurora Focus, combines a Behavioral Detection Engine with AI-assisted analysis to provide endpoint visibility and automated response capabilities.

System Architecture

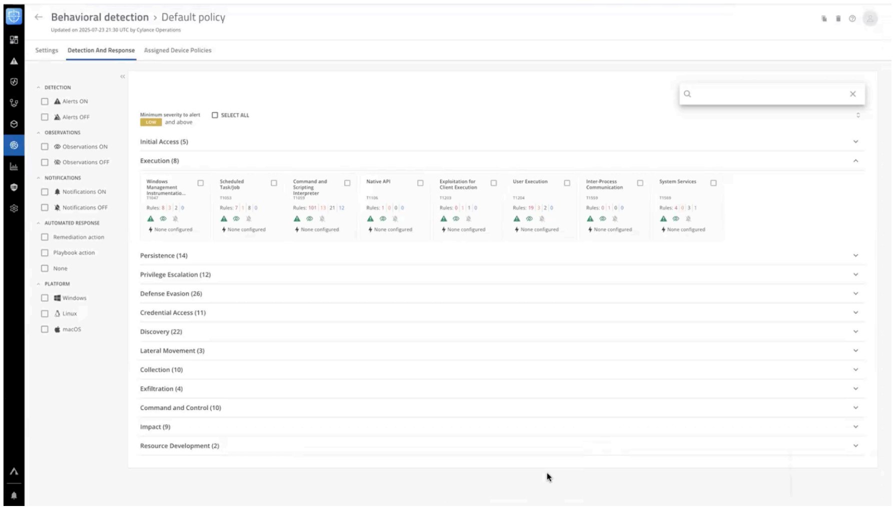
Aurora Focus deploys behavioral detection policies directly to endpoints, maintaining protection during offline operation. The system correlates multiple detections into consolidated alerts and provides MITRE ATT&CK framework[1] mappings for each detection. An embedded AI assistant analyzes command-line arguments and provides contextual information for detected behaviors.

Testing Methodology

Tolly evaluated Aurora Focus using a multi-stage cyberattack simulation replicating common threat actor tactics: encoded PowerShell execution, payload staging, MSHTA UAC bypass, LSASS credential dumping, scheduled task persistence, Windows event log clearing, and BitAdmin data exfiltration.

Testing utilized two identical endpoints: one configured in observability mode (detection only) and another with autonomous response actions enabled. This configuration allowed measurement of both detection coverage and response effectiveness.

Aurora Endpoint Defense
Behavioral Detection Dashboard



Behavioral detection > Default policy
Updated on 2025-07-23 21:30 UTC by Cylance Operations

Settings | Detection And Response | Assigned Device Policies

DETECTION
□ Alerts ON
□ Alerts OFF
OBSERVATIONS
□ Observations ON
□ Observations OFF
NOTIFICATIONS
□ Notifications ON
□ Notifications OFF
AUTOMATED RESPONSE
□ Remediation action
□ Playbook action
□ None
PLATFORM
□ Windows
□ Linux
□ macOS

Minimum severity to alert: LOW and above
□ SELECT ALL

Initial Access (5)

Execution (8)

Technique	ID	Rules	Response
Windows Management Instrumentatio...	T1047	8 | 3 | 2 | 0	None configured
Scheduled Task/Job	T1053	7 | 1 | 8 | 0	None configured
Command and Scripting Interpreter	T1059	101 | 13 | 21 | 12	None configured
Native API	T1106	1 | 0 | 0 | 0	None configured
Exploitation for Client Execution	T1203	0 | 1 | 1 | 0	None configured
User Execution	T1204	19 | 3 | 2 | 0	None configured
Inter-Process Communication	T1559	0 | 1 | 0 | 0	None configured
System Services	T1569	4 | 0 | 3 | 1	None configured

Persistence (14)
Privilege Escalation (12)
Defense Evasion (26)
Credential Access (11)
Discovery (22)
Lateral Movement (3)
Collection (10)
Exfiltration (4)
Command and Control (10)
Impact (9)
Resource Development (2)

Source: Tolly, August 2025 Figure 3

Test Results

Detection Coverage

To illustrate the multi-layer capability of Aurora Focus the policy was deliberately set to Alert for recording purposes. The system successfully identified all attack stages in observability mode, documenting the complete attack chain from initial PowerShell execution through data exfiltration attempts. Malicious payloads were automatically quarantined upon detection. For a visual flow of the alerts triggered during the attack, see Figure 4.

Response Performance

With autonomous response enabled, the system terminated the encoded PowerShell process at initial execution, preventing all subsequent attack activities. Response actions included process tree termination and playbook execution for evidence collection.

Offline Capability

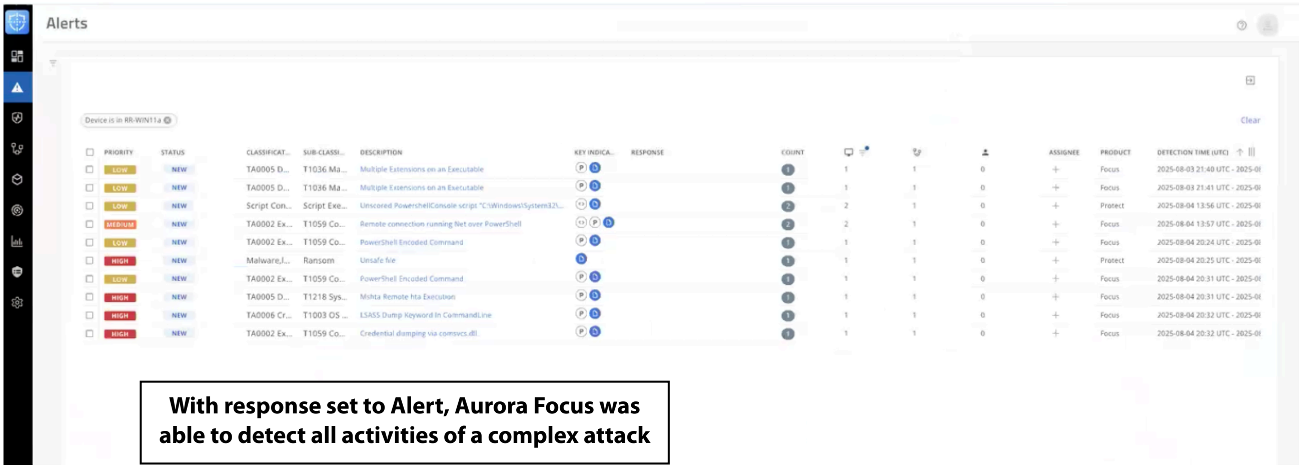
All detection and response functions operated independently of cloud connectivity, confirmed through network disconnection testing.

AI Analysis

The embedded AI assistant provided technical explanations of detected behaviors and MITRE framework mappings without requiring external queries.

[1] https://attack.mitre.org/

Aurora Endpoint Defense
Alert Flow for Complex Threat



☐	PRIORITY	STATUS	CLASSIFICAT...	SUB-CLASSI...	DESCRIPTION	KEY INDICA...	RESPONSE	COUNT				ASSIGNEE	PRODUCT	DETECTION TIME (UTC)
☐	LOW	NEW	TA0005 D...	T1036 Ma...	Multiple Extensions on an Executable	P		1	1	1	0	+	Focus	2025-08-03 21:40 UTC - 2025-0
☐	LOW	NEW	TA0005 D...	T1036 Ma...	Multiple Extensions on an Executable	P		1	1	1	0	+	Focus	2025-08-03 21:41 UTC - 2025-0
☐	LOW	NEW	Script Con...	Script Exe...	Unscored PowershellConsole script "C:\Windows\System32\...			2	2	1	0	+	Protect	2025-08-04 13:56 UTC - 2025-0
☐	MEDIUM	NEW	TA0002 Ex...	T1059 Co...	Remote connection running Net over PowerShell	P		2	2	1	0	+	Focus	2025-08-04 13:57 UTC - 2025-0
☐	LOW	NEW	TA0002 Ex...	T1059 Co...	PowerShell Encoded Command	P		1	1	1	0	+	Focus	2025-08-04 20:24 UTC - 2025-0
☐	HIGH	NEW	Malware,I...	Ransom	Unsafe file			1	1	1	0	+	Protect	2025-08-04 20:25 UTC - 2025-0
☐	LOW	NEW	TA0002 Ex...	T1059 Co...	PowerShell Encoded Command	P		1	1	1	0	+	Focus	2025-08-04 20:31 UTC - 2025-0
☐	HIGH	NEW	TA0005 D...	T1218 Sys...	Mshta Remote hta Execution	P		1	1	1	0	+	Focus	2025-08-04 20:31 UTC - 2025-0
☐	HIGH	NEW	TA0006 Cr...	T1003 OS ...	LSASS Dump Keyword In CommandLine	P		1	1	1	0	+	Focus	2025-08-04 20:32 UTC - 2025-0
☐	HIGH	NEW	TA0002 Ex...	T1059 Co...	Credential dumping via comsvcs.dll	P		1	1	1	0	+	Focus	2025-08-04 20:32 UTC - 2025-0

With response set to Alert, Aurora Focus was able to detect all activities of a complex attack

Source: Tolly, August 2025

Figure 4

Test Setup & Methodology

Environment

All testing was run using Windows 11 Pro 2024H2 64-bit systems running in a virtualized environment under Windows Azure. The Azure VM type was a Standard D2s_v3. All Windows systems were updated with updates available as of August 2025. After the updates were applied the automatic update function was paused to avoid any changes to the systems while testing.

The virtual machine was configured with a 2.3GHz Intel Xeon processor (1 core, 2 vCPUs), 8GB of RAM, and 16GB of storage. Internet connectivity was provided by a virtualized Gigabit Ethernet network adapter. Windows Defender and other built-in security features are automatically disabled when Aurora Endpoint Security is running, helping to avoid interference with test results.

The Aurora Protect & Focus agents tested were version 3.4.1000. A stabilization period lasting 4 hours was observed post-installation to ensure all background threat detection processes were completed.

Solution Installation

Each solution tested provided a cloud-managed administration environment. For each solution, the Windows installer was downloaded to onboard the endpoint.

A typical enterprise policy setting was configured for the test environments. For full details on the settings utilized, see Table 1.

Network Test Environments

Tests were run with the Windows system default configurations with Internet connectivity enabled.

The endpoint protection solution was thus able to query its centralized threat database when reaching a verdict on a threat, in addition to its local resources and on-device threat detection and elimination capabilities.

Malware Samples

All malware samples were downloaded from major public sources. The sample set consisted of 1,000 files classified by major public sources as malware.

A compressed (ZIP), password-protected file of approximately 1GB was produced for the test. The file was password protected so that engineers could trigger the start of the scan manually.

Test Process

Malware samples were copied to the endpoint solution under test. The network connection was enabled/disabled as required by the scenario. Engineers opened the Microsoft Resource Monitor window on the Windows system under test, and separately started a perfmon script, which allowed engineers to monitor system performance on one second intervals.

Start time was recorded as the time that the password was typed in and the "extract all" command began to process. End time was recorded as the time when the endpoint processes ceased removing files from the test malware folder.

As the target folders contained 1,000 samples of malware, a perfect score would leave zero files remaining in the target folder. The number of files remaining in the target folder was used to calculate the threat detection percentage.

Two separate test runs were conducted using different 1,000-sample subsets from major public sources to verify repeatability, with CPU utilization results varying by less than 5% and detection rates maintaining consistency across runs.

Test Validation

Test results were validated through multiple verification methods including log file analysis, system event correlation, and manual verification of quarantined file counts. All test procedures were documented and repeatable to ensure scientific rigor.

Aurora Endpoint Security Policy Settings

Policy Section	Policy Key	Policy Value
File Actions	Auto Block	Enabled
	Executable Auto Upload	Disabled
Memory Actions	Memory Protection	Enabled
	Exclude Executable Files	Disabled
	(Remainder of Memory Actions)	Terminate
Protection Settings	Prevent Service Shutdown From Device	Enabled
	Kill Unsafe Processes & Sub-Processes	Enabled
	Background Threat Detection	Run Once
	Watch For New Files	Enabled
	Maximum Archive File Size to Scan	150mb
	Exclude Specific Folders	Enabled
	Allow Execution	Enabled
	Copy File Samples	Disabled
	Application Control	Disabled
Agent Settings	Enable Auto-Upload of Log Files	Disabled
Script Control	Script Control	Enabled
	All Scripts (ex. PowerShell)	Block
	PowerShell Scripts[1]	Alert
Device Control	Device Control	Disabled
Data Privacy	Data Privacy	Disabled

[1] PowerShell scripts remained activated for perfmon recording purposes only.

Source: Tolly, August 2025

Table 1

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 35 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

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

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

bu-1-wt-2025-08-12—VerF