



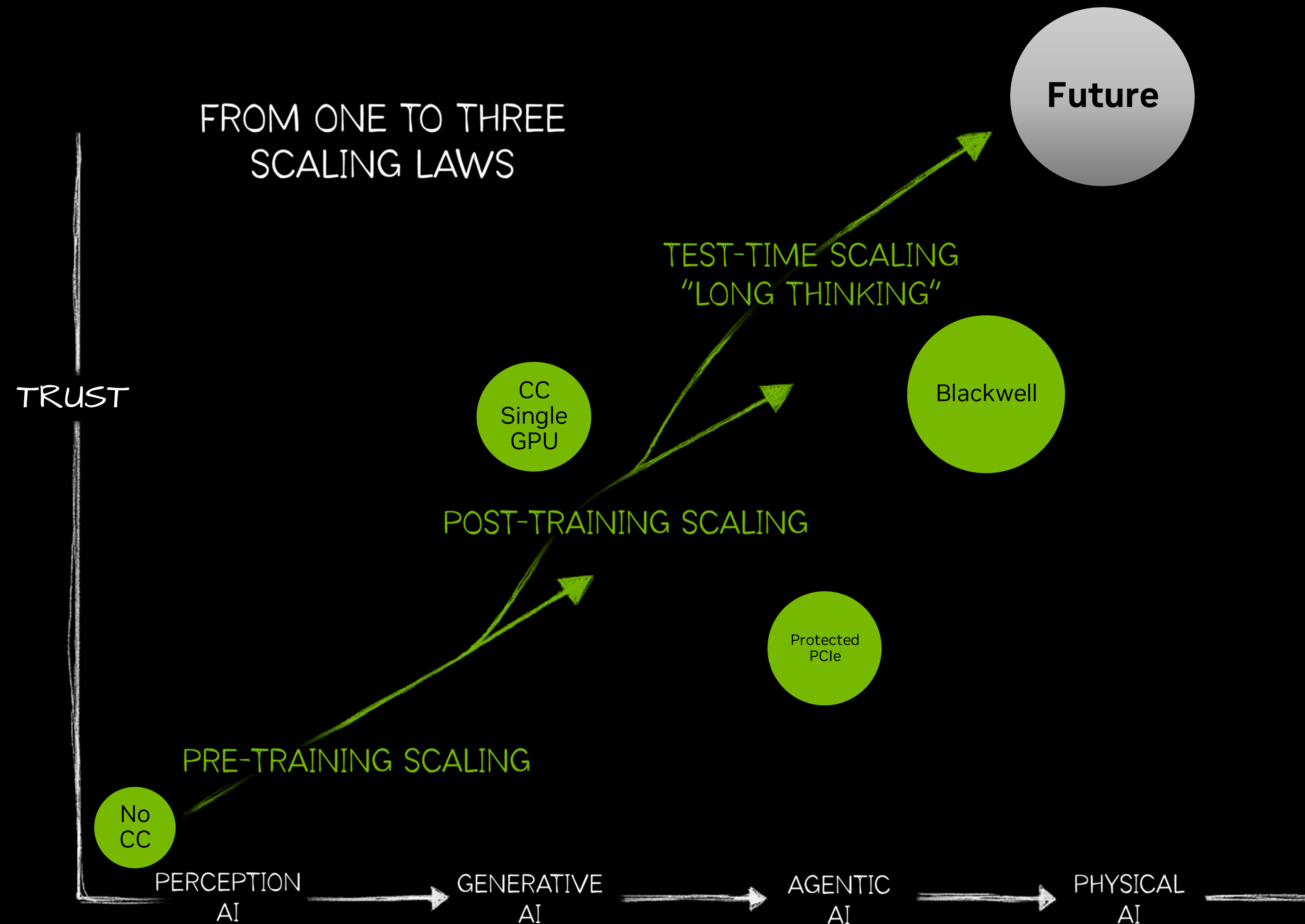
# Securing AI's Third Dimension: Scaling Trust for Autonomous Intelligence

Daniel Rohrer, VP Product Security | OC3 – 2025



# Responding to Changing Landscape

## Three Scaling Laws and Scaling Trust for New Workloads





# Delivering a Secure Foundation for the Future of AI

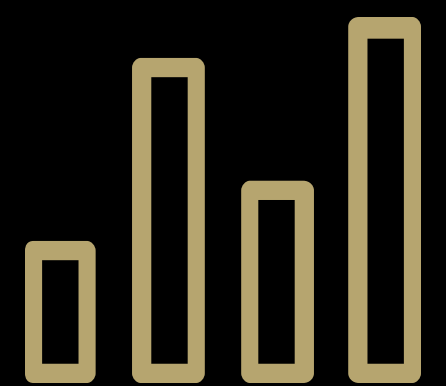
Join the Trusted AI Revolution



Security



Performance



Scale





# Transforming Industries Through Trusted AI

Regulatory Compliance without Compromise



USER SERVICES

# Transforming Industries Through Trusted AI

Regulatory Compliance without Compromise



HEALTHCARE & LIFE  
SCIENCES



USER SERVICES



FINANCIAL SERVICES



# Transforming Industries Through Trusted AI

Regulatory Compliance without Compromise



EMERGING



HEALTHCARE & LIFE  
SCIENCES



USER SERVICES



FINANCIAL SERVICES

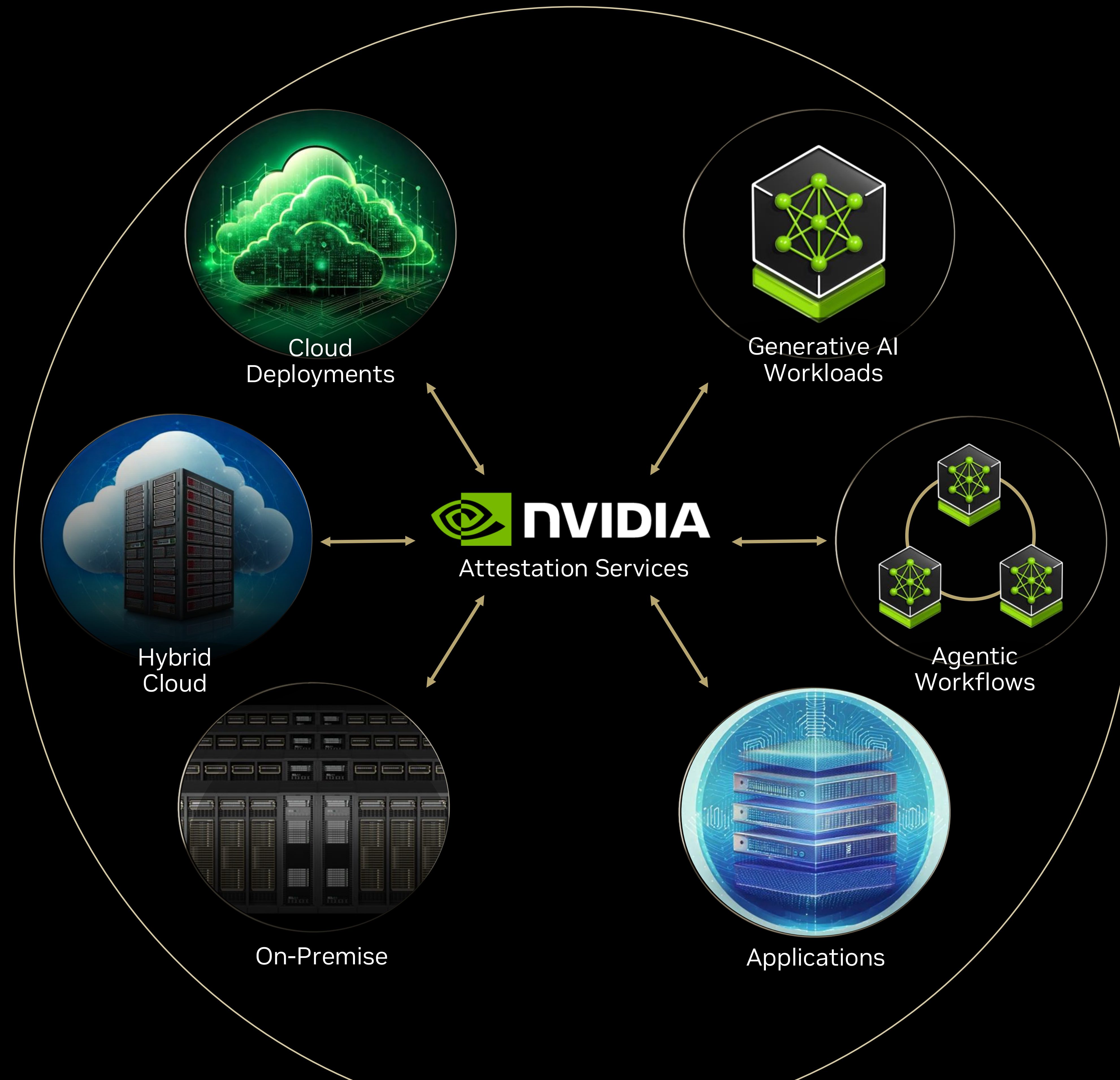


PUBLIC SECTOR



# Building Trust Through Verification

Attestation and Trusted Tokens





# Building Trust for the Future of Autonomous AI

Security and Trust to Meet the Needs of the Modern AI Factory









# DISCLOSURES

- **Forward Looking Statements.** Information on (or linked to) the Site, other than statements or characterizations of historical fact, may contain forward-looking statements. These forward-looking statements are based on our current expectations, estimates and projections about our industry, management's beliefs and certain assumptions made by us. These forward-looking statements are subject to a number of significant risks and uncertainties and our actual results may differ materially. For a discussion of factors that could affect our future results and business, please refer to our Annual Report on Form 10-K, subsequent Quarterly Reports on Form 10-Q, recent Current Reports on Form 8-K, and other Securities and Exchange Commission filings. NVIDIA undertakes no obligation to revise or update any forward-looking statements.
- **Trademark Information.** © 2025 NVIDIA Corporation. All rights reserved. NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated. You may not use NVIDIA's trademarks without NVIDIA's prior written permission, and nothing in these Terms shall be construed as granting such permission. Fair use of NVIDIA's trademarks in advertising and promotion of NVIDIA products requires proper acknowledgment.
- **Performance Information.** Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of NVIDIA products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance.