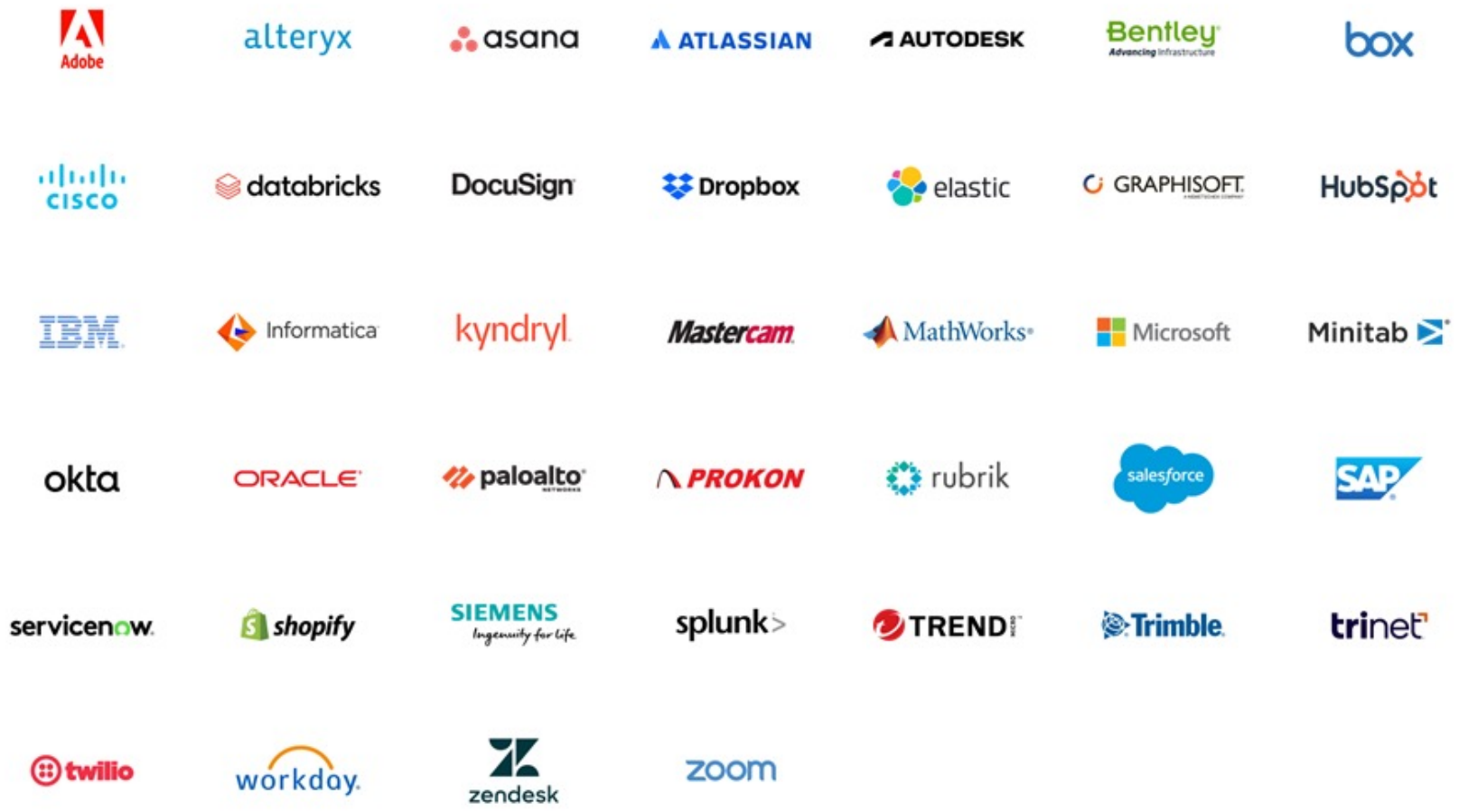
CYBERSECURITY FOR GENERATIVE AI

Leveraging Existing Tools and Identifying New Challenges

BSA | The Software Alliance



TRADITONAL AND GENERATIVE AI SYSTEMS

- Hardware
- Software
- Impact

SOFTWARE SECURITY

The BSA Framework for Secure Software

NIST Secure Software Development Framework

IDENTIFYING NEW GAPS

- Purpose
- Adaptability
- Data Dependency
- Complexity
- Autonomy

NEXT STEPS

- Reassert a risk management approach
- Educate policymakers, business leaders, and software developers
- Identify needs through public-private partnerships
- Create additional guidance as needed
- Standardize

CYBERSECURITY FOR GENERATIVE AI

Leveraging Existing Tools and Identifying New Challenges