

CYBERSECURITY FOR GENERATIVE AI

Leveraging Existing Tools and
Identifying New Challenges



BSA | The Software Alliance



alteryx

asana

ATLASSIAN

AUTODESK

Bentley
Advancing Infrastructure

box



databricks

DocuSign

Dropbox

elastic

GRAPHISOFT

HubSpot



Informatica

kyndryl

Mastercam

MathWorks

Microsoft

Minitab

okta

ORACLE

paloalto

PROKON

rubrik



SAP

servicenow

shopify

SIEMENS
Ingenuity for Life

splunk

TREND

Trimble

trinet

twilio

workday

zendesk

zoom

TRADITIONAL 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

