CISA SBOM CLOUD STACK TRANSPARENCY

Bhargav Vivekanandan
Andre Koot
Rene Pluis
Asaf Atzmon
Doug Cavit

AGENDA

- Mission
- Summary
- Deliverables
- Future
- Community Outreach

MISSION

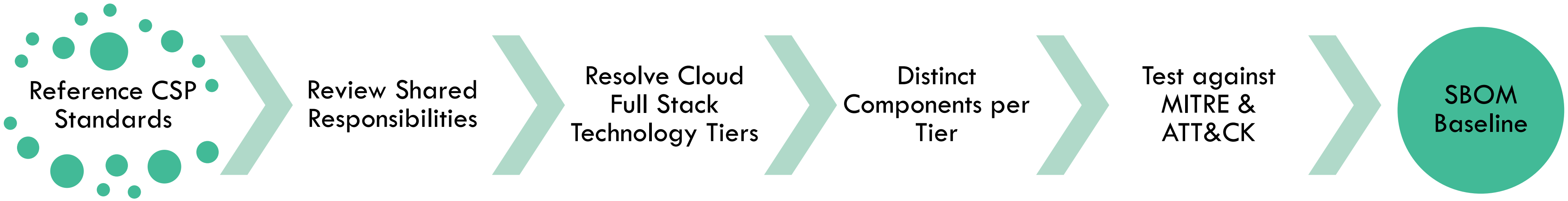
Contribute to the development of an **industry standard for the implementation of SBOM for the cloud**

Develop a solution that can be applied to all types of cloud deployment models including public, private and hybrid as well as cloud services including but not limited to **Infrastructure As A Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)**

A global standard that can be adopted by any industry and by **consumers and cloud service providers (CSP) alike**

Brand agnostic coverage of the full technology stack from the application tier to the bare metal tier

SUMMARY



Reference CSP Standards

Review Shared Responsibilities

Resolve Cloud Full Stack Technology Tiers

Distinct Components per Tier

Test against MITRE & ATT&CK

SBOM Baseline

- Min Required SBOMs
- Use Cases & Benefits

DELIVERABLES

A publication on the SBOM Cloud Stack Transparency that addresses the following,

1. **Thought process** behind the solution development

2. The **significance of the shared responsibilities matrix** for cloud service types

3. **Cloud technology stack derivation** from the reference architecture

4. Table of **minimum required distinct technology components per technology tier**

5. **Use Cases and relationships** with the larger SBOM solution development streams

FUTURE PLANS & COMMUNITY OUTREACH

- A round of iteration with stakeholders and socialization with the larger CISA SBOM community
- Community outreach to major CSP representatives via CISA
- Finalize iteration and test against MITRE and ATT&CK
- Iron out issues if any and close final iteration
- Publish the best practice/guideline on SBOM Cloud Stack Transparency

THANK YOU

Q&A

Service Transparency

Mission

- Describe an initial list of fields describing a “Software Service”
  - Scope down to an online or running service sending and receiving network calls
- Deliver a whitepaper
  - Motivation
  - Fields
  - Gaps
- Identify gaps in knowledge and document possible future work

Topics Discussed

- Use cases
    - In Scope/Out of Scope
    - Data needed to address use cases
- Narrowing of scope
    - What we know and what we don’t know
    - What is “software component” and what is “software service” (layer 7)
    - Direct vs Transitive Service Dependencies
    - Distance from “SBOM”
- Reaching consensus
    - Time bound discussions
    - Specific questions
    - Real world “test fixtures”

Deliverable and Community Asks

- Please review the whitepaper draft and provide feedback: google doc
- We need “test fixtures”
  - Scenarios
  - Edge cases
- We need more work on Future Work
  - Need experts in Data Governance, Service Availability, and Observability

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

WG: SBOM Cloud

Subgroup: SBOM Classic for Modern Applications

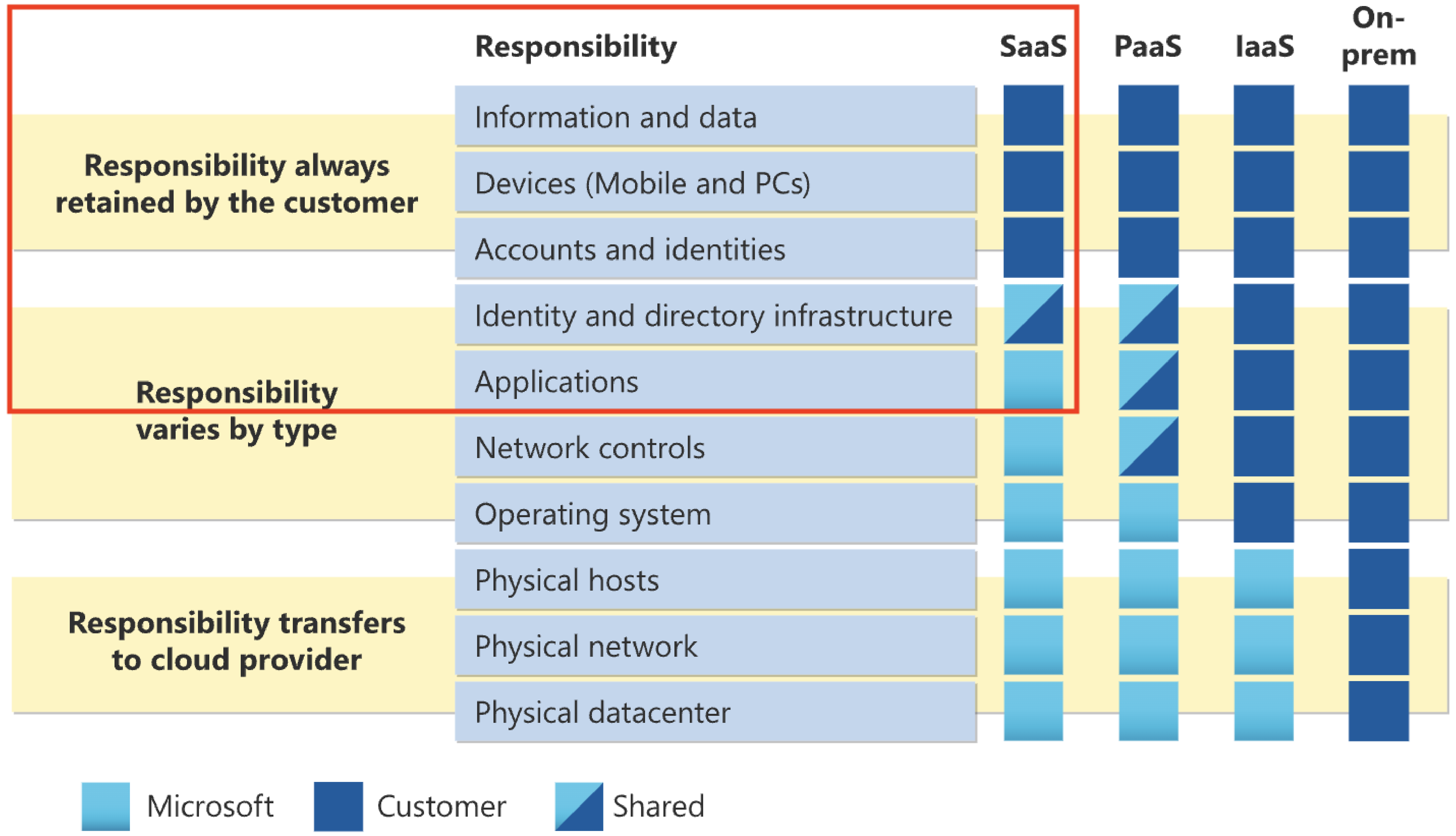
Chair: Ricardo A. Reyes
Sr. Solutions Architect
ricardo@tidelift.com
TIDELIFT

Co-Chair: Deanna Medina
Cybersecurity Architect/Engineer
deanna.medina@honeywell.com
Honeywell

SBOM for Software as a Service (SaaS)

Software as a service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. SaaS is also known as on-demand software, web-based software, or web-hosted software.

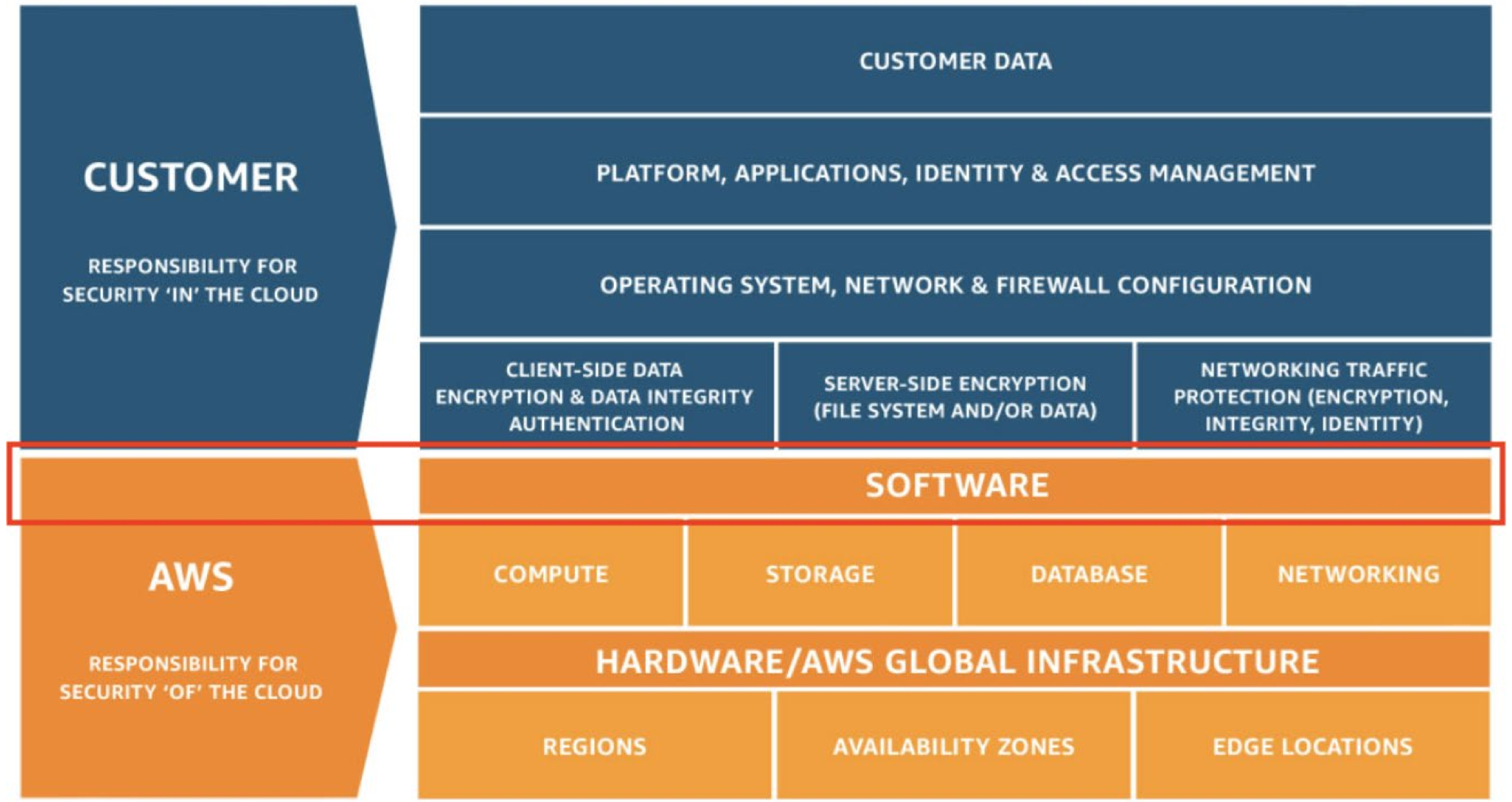
Cloud shared responsibility model



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

Source: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

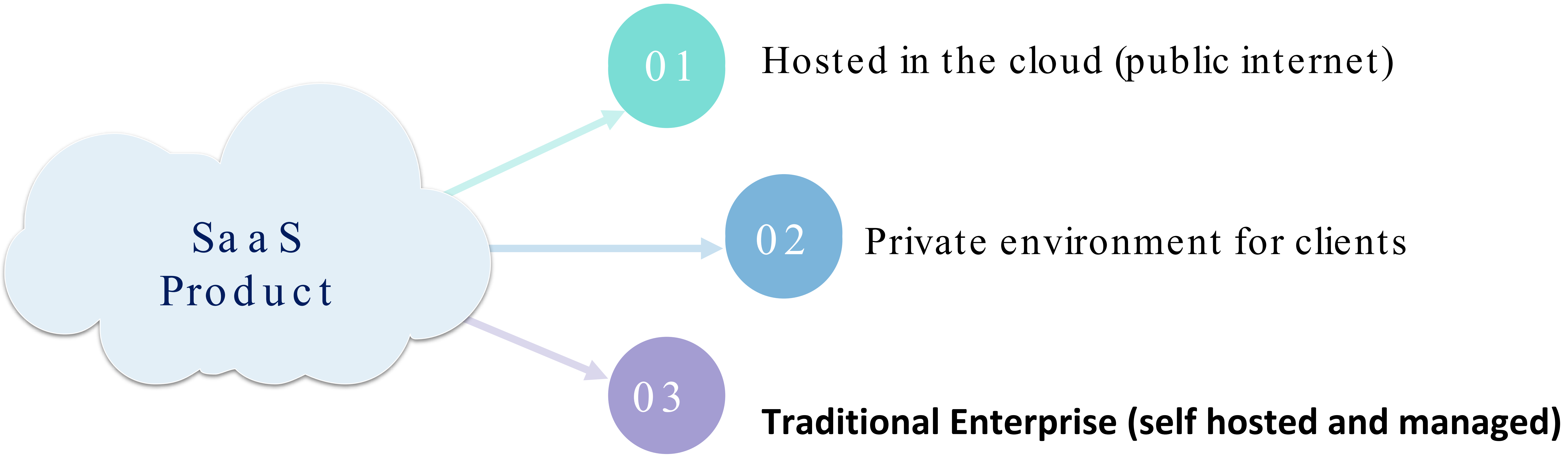
AVAILABILITY ZONES

EDGE LOCATIONS

Source: https://aws.amazon.com/compliance/shared-responsibility-model/

Focus: SBOM and SaaS in the Cloud and On-Premises Environments

Provide a comprehensive overview of SBOM for SaaS hosted in the Cloud and On-prem for identifying vulnerable components/ libraries, risk factors, and fortifying the software ecosystem against potential threats.



Hosted in the cloud (public internet)

Private environment for clients

Traditional Enterprise (self hosted and managed)

SaaS vendors SBOM responsibilities

Businesses owners shall make SBOM requests from SaaS service providers

SaaS Product

Providers

SaaS providers
issue an SBOM

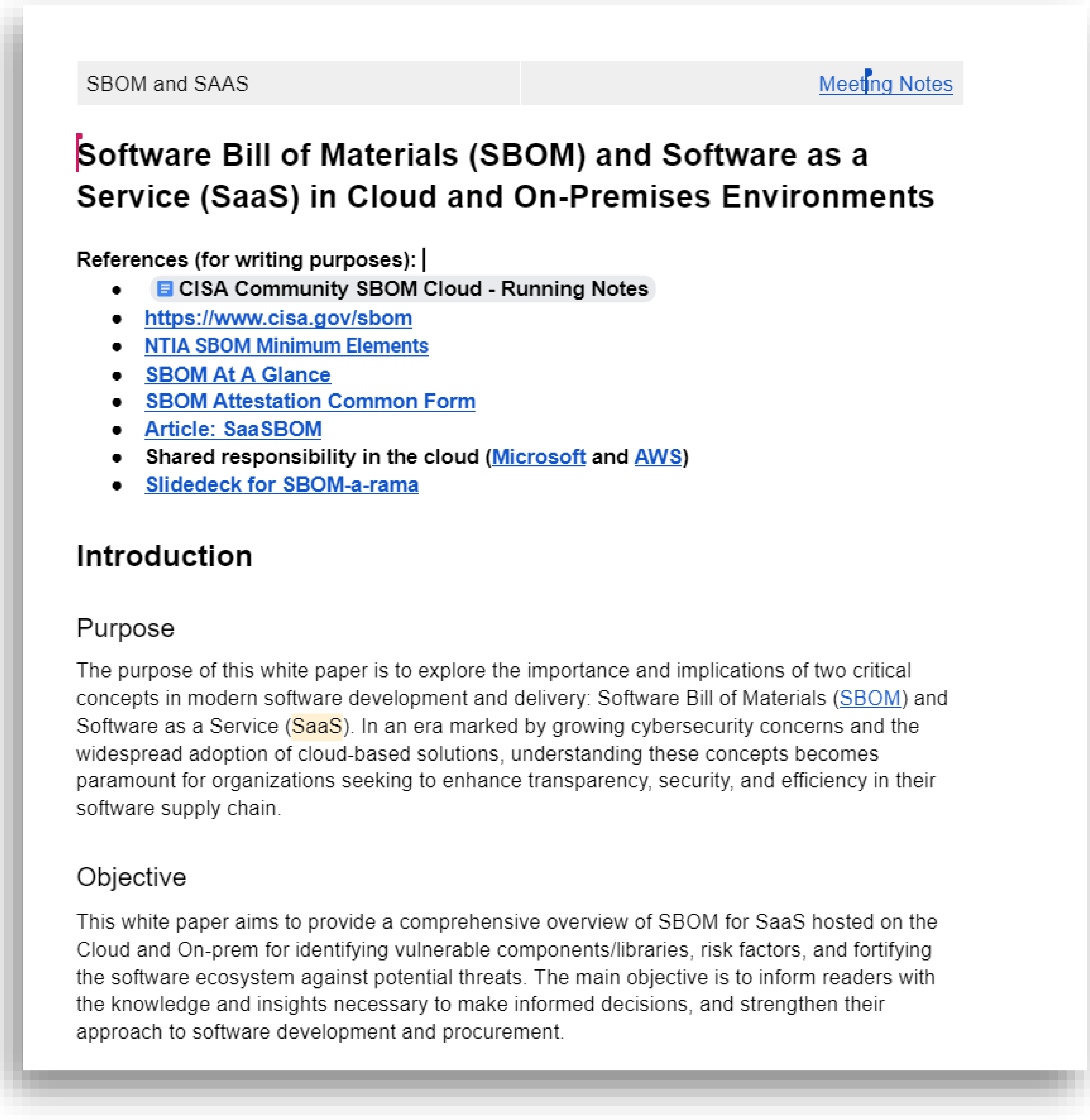
Customers

Businesses owners
request an SBOM

White Paper

Outline

- **Introduction**
- **SaaS vs Software On-premises**
  - Why is SaaS different with respect to SBOM
    - Velocity of code base
    - Limited customer/user actions / mitigation /control options
    - Limited visibility into versioning and updates
    - SAAS architecture concepts are better defined
    - Blast radius is bigger
    - SaaS is often customized for specific customers, customer needs
    - Reverse-engineering on prem software might be more difficult for SaaS
  - Why is SAAS not really different
  - Other considerations
- **Paths for implementing SBOM requirement for SAAS**
  - Spectrum for SBOM delivery
    - No SBOM
    - Assert/attest SBOM exists
    - Snapshot of SBOM when making procurement/contract decisions
    - Live or SBOM on demand
    - VEX
    - Why are we doing this?
- **Recommendations**



SBOM and SAAS | Meeting Notes

Software Bill of Materials (SBOM) and Software as a Service (SaaS) in Cloud and On-Premises Environments

References (for writing purposes):

- CISA Community SBOM Cloud - Running Notes
- https://www.cisa.gov/sbom
- NTIA SBOM Minimum Elements
- SBOM At A Glance
- SBOM Attestation Common Form
- Article: SaaSBOM
- Shared responsibility in the cloud (Microsoft and AWS)
- Slidedeck for SBOM-a-rama

Introduction

Purpose

The purpose of this white paper is to explore the importance and implications of two critical concepts in modern software development and delivery: Software Bill of Materials (SBOM) and Software as a Service (SaaS). In an era marked by growing cybersecurity concerns and the widespread adoption of cloud-based solutions, understanding these concepts becomes paramount for organizations seeking to enhance transparency, security, and efficiency in their software supply chain.

Objective

This white paper aims to provide a comprehensive overview of SBOM for SaaS hosted on the Cloud and On-prem for identifying vulnerable components/libraries, risk factors, and fortifying the software ecosystem against potential threats. The main objective is to inform readers with the knowledge and insights necessary to make informed decisions, and strengthen their approach to software development and procurement.

Contributors

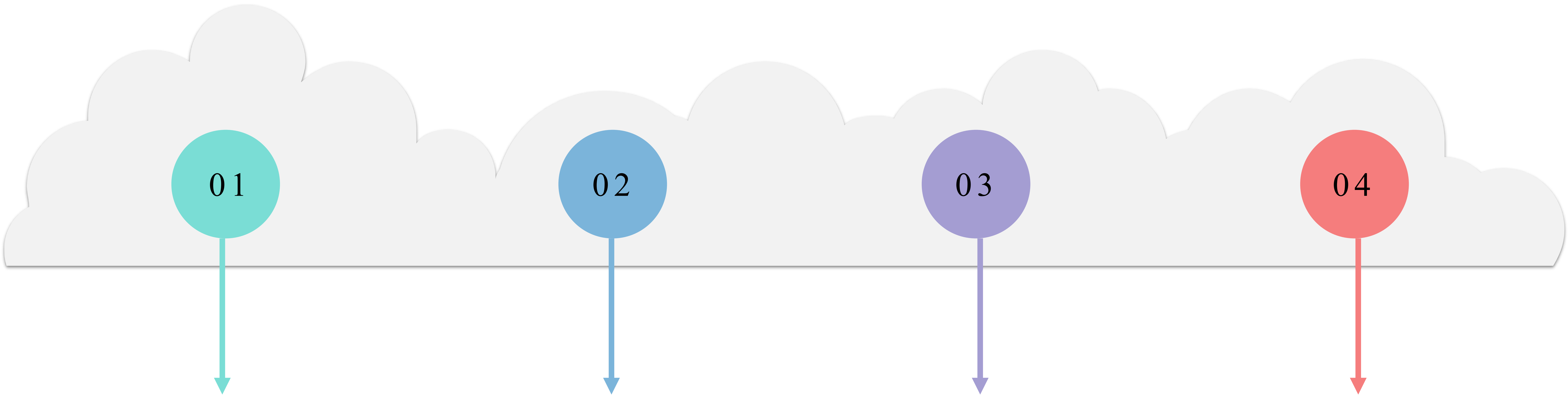
Aditi Sharma, Dell
Adrian Diglio, Microsoft
Aiden Clark, Iconist.us
Allan Friedman, CISA
Allen Smith, Umbraco.com
Bamidele Odeniyi, BAH
Ben Prime, ServiceNow
Craig Rubin, HPE
Courtney Robertson, GoDaddy
David, Cybellum.com,
Douglas Cavit, Cavit.net
Emily Fesnak, Deloitte
Gray Williams, ServiceNow

Henri Yandell, AWS
Jason Beland, ServiceNow
Jefferson Lacorte, ServiceNow
Jeremiah T. Stoddard, INL.gov
John K, Launchdarkly.com
Jonathan Alboum, ServiceNow
Lon Shapiro, ACM.org
Maulik Shah, ServiceNow
Michael Greco, ServiceNow
Mike Rohde, ServiceNow
Minatee Mishra, Philips
Mike Thompson, AWS

Nisha Kumar, Oracle
Omar, Cloudflare
Paul Giorgi, Xmcyber.com
Paula Paul, Nearform.com
Rene Pluis, Philips
Russell, Edgebit.io
Ryan Doughty, ServiceNow
Sandeep Patil, Philips
Shafia Zubair, Johnson Controls
Simon Lokhvidson, Avmltd.com
Steve Springett, ServiceNow
Trevi Housholder, DocuSign
Vincent Stammegna ServiceNow

Subgroup Challenges

A lot of industry diversity to bring together



01

Diversity

Wide perspective from all tech industries

02

Scope

Deep and broad subject area for SBOM and SaaS

03

Collaboration

A volunteer effort, finding momentum and continuous engagement

04

Terminology

Evolving landscape

SG: SBOM Classic for Modern Applications

Weekly meetings discussions on Fridays and White Paper contribution asynchronous.

Zoom Meetings

Fridays 12 - 1:00 PM EDT

Meeting Minutes

White Paper