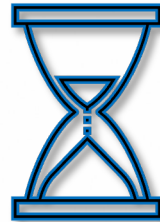


# FedRAMP

The **Federal Risk and Authorization Management Program (FedRAMP)** is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.



Mandatory certification to **offer cloud services** to US Federal Government



FedRAMP can be **resource intensive and expensive**

# FedRAMP Challenges



Building a **compliant system** for federal customers can be challenging, resource intensive, and time consuming



Requires **hiring additional resources** for FedRAMP-related activities\*



**Maintaining and managing** the authorized environment is a significant investment

\*Dedicated resources should be considered due to work for teams supporting FedRAMP activities. Different sponsor agencies may have unique/stringent requirements (e.g., US-based resources).



## FedRAMP Requirements

Infrastructure Stack

Monitoring Stack

Identity & Access Stack

Process & Workflow

Gov Version of Application; feature parity with the commercial version



Operational & Security Controls



Engineering Controls

Implement

Operate

Implement

Operate



Monitor

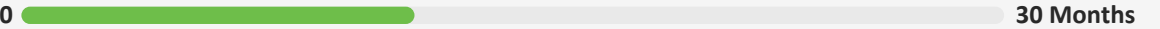
# Accelerate Product FedRAMP Timeline with Federal Ops Stack

## Traditional Approach

0  30 Months

Ready for Audit in **~24 Months +**

## Using Federal Ops Stack

0  30 Months

Ready for Audit in **~12 Months**


### Product | Effort Analysis

 Solely maintain authorization (monthly and annual audits, documentation etc.)

 Sole responsibility to address all 325 controls

#### FedRAMP Controls

 Operational & Security Controls

 Engineering Controls

Implement

Operate


Implement


Operate


Monitor

Total = 325 Controls (Rev4)


### Ops Stack | Effort Analysis


 Leverage FedRAMP-compliant Operational Security stack of services/tools

 Offload implementation of engineering-heavy technical controls

 Benefit from Ops stack offered heavy lifting for **maintaining the certification post-authorization**

#### FedRAMP Control Stack

 Operational & Security Controls

 Engineering Control Stack

Implement

Operate

Implement

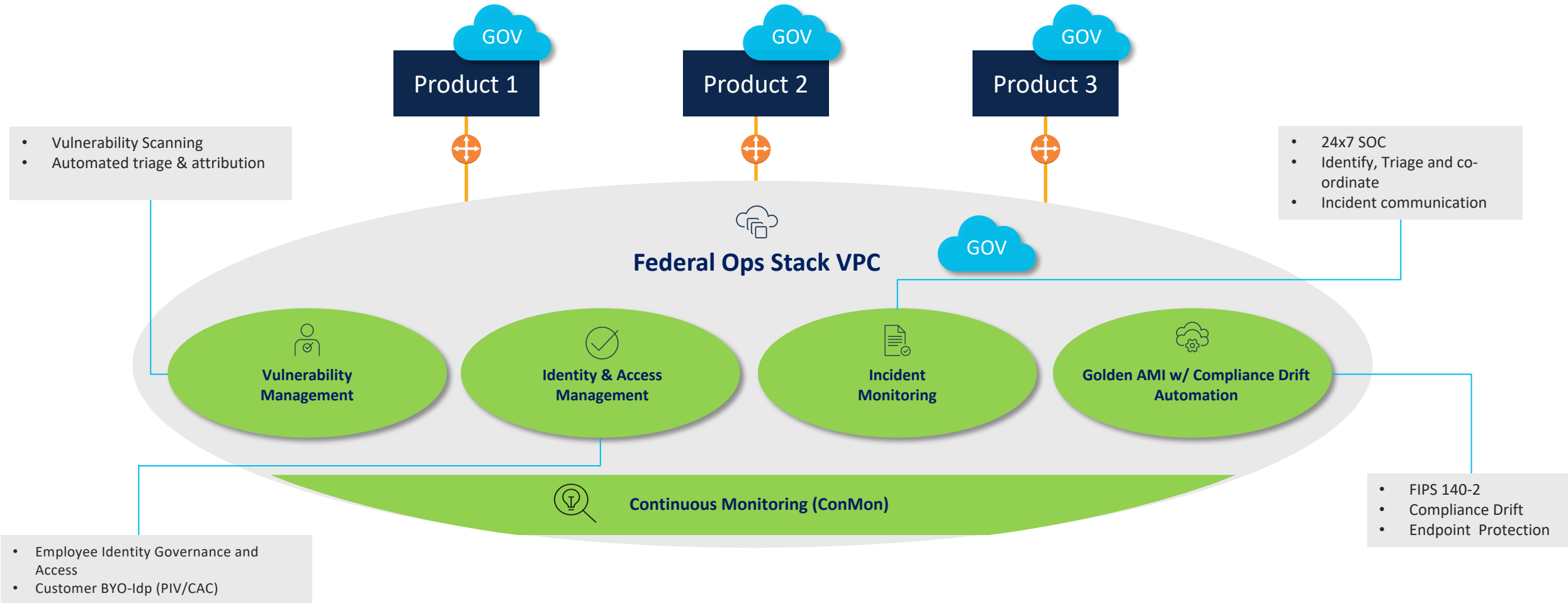
Operate

Monitor

Ops Stack inherited controls ~40-60%

Total = 325 Controls (Rev4)

# Federal Ops Stack Services: Services and Key Features



# Federal Ops Stack: Services & Tools: IAM



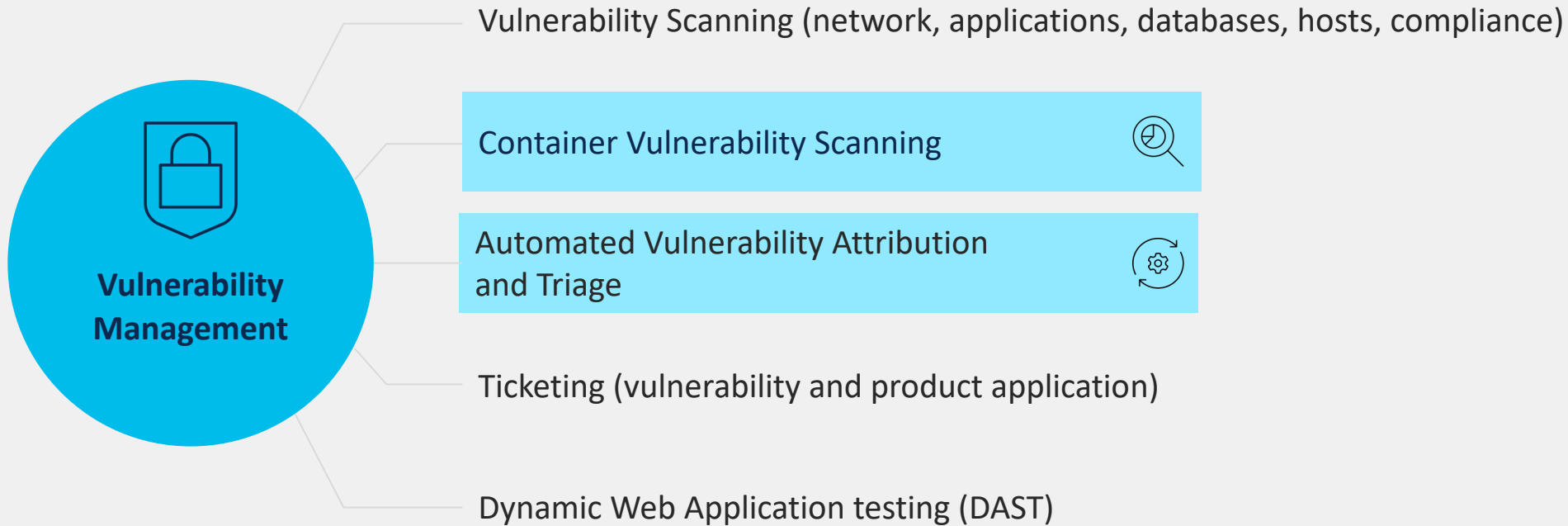
## Service Components



# Federal Ops Stack: Services & Tools: Vulnerability Management



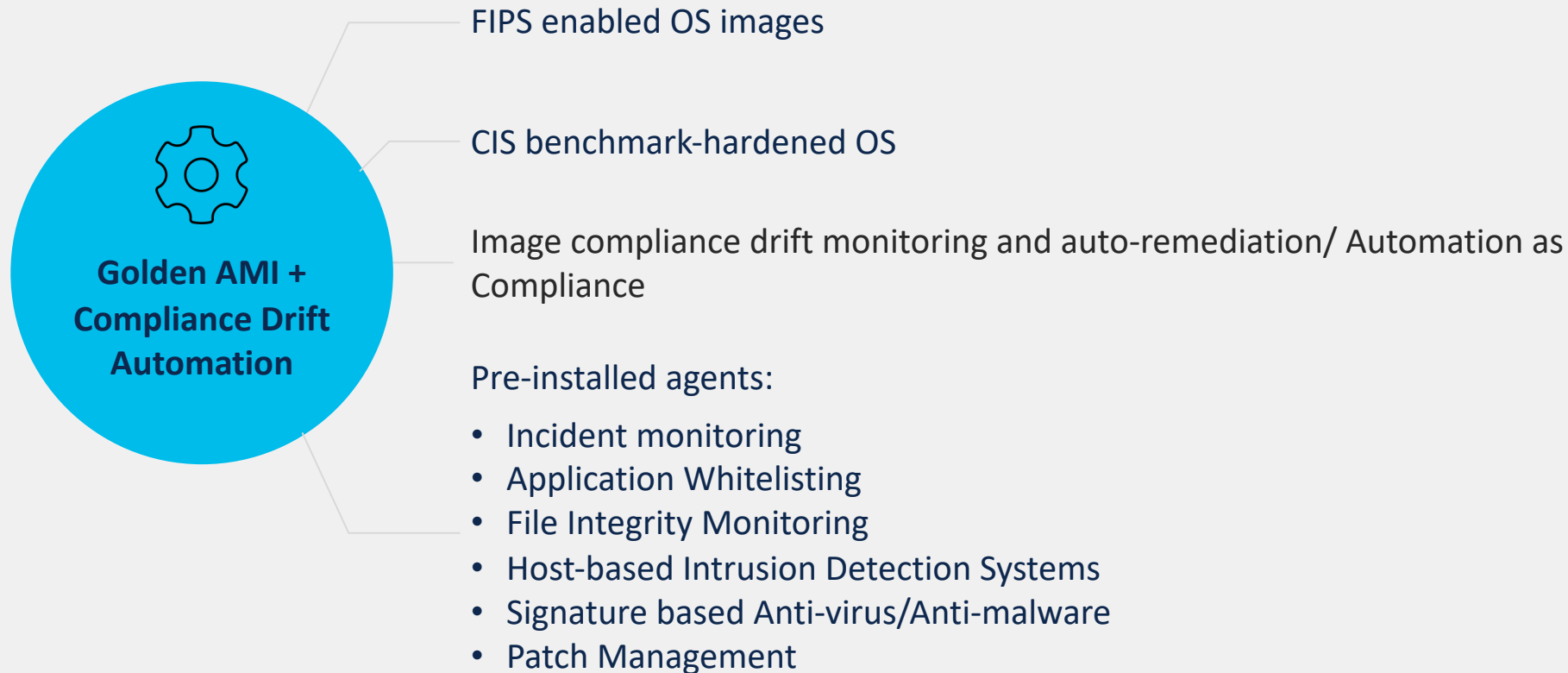
## Service Components



# Federal Ops Stack: Services & Tools: Golden AMI w/ Compliance Drift Monitoring and Remediation



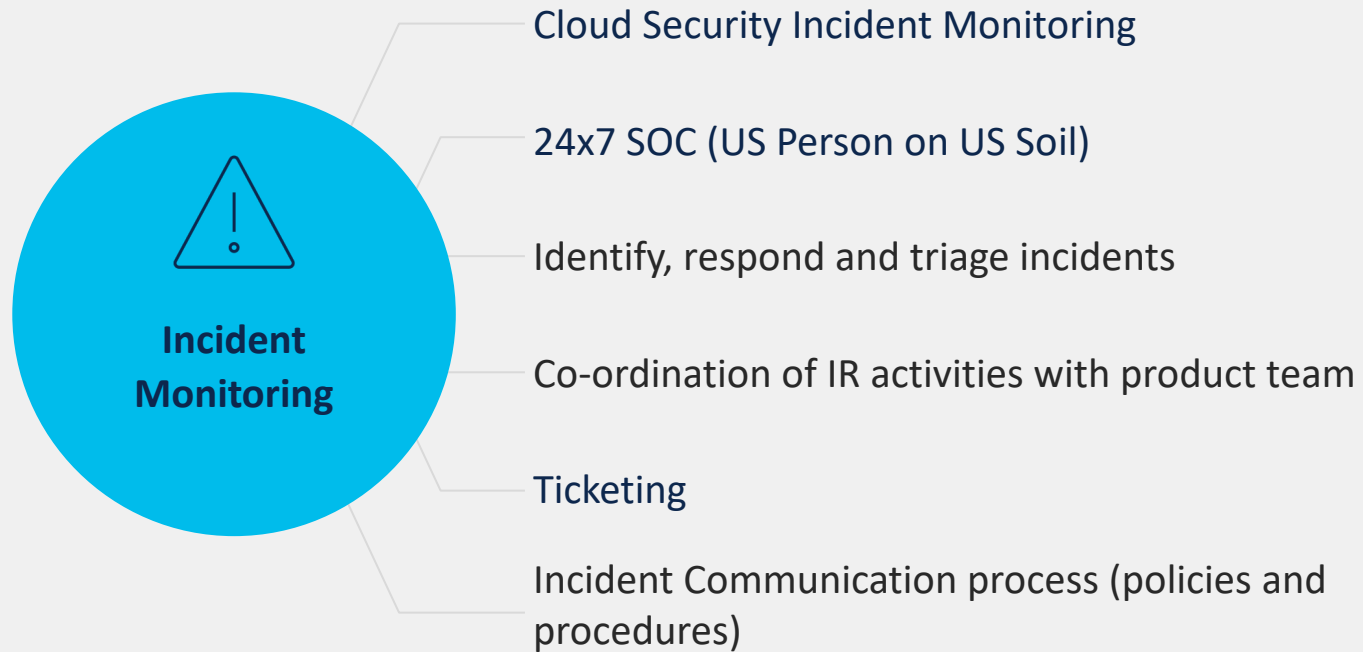
## Service Components



# Federal Ops Stack: Services & Tools: Incident Monitoring



## Service Components





# Federal Ops Stack: Services & Tools: Continuous Monitoring

**Monthly ConMon Activities**

- Vulnerability scans
- Plan of Actions and Milestones (POA&M) entries
- Deviation Requests
- Executive Summary for authorizing official
- FedRAMP Inventory update

**Annual Assessments**

- Request for information/evidence
- Pen Test Assistance
- Interview preparations
- Remediation scans

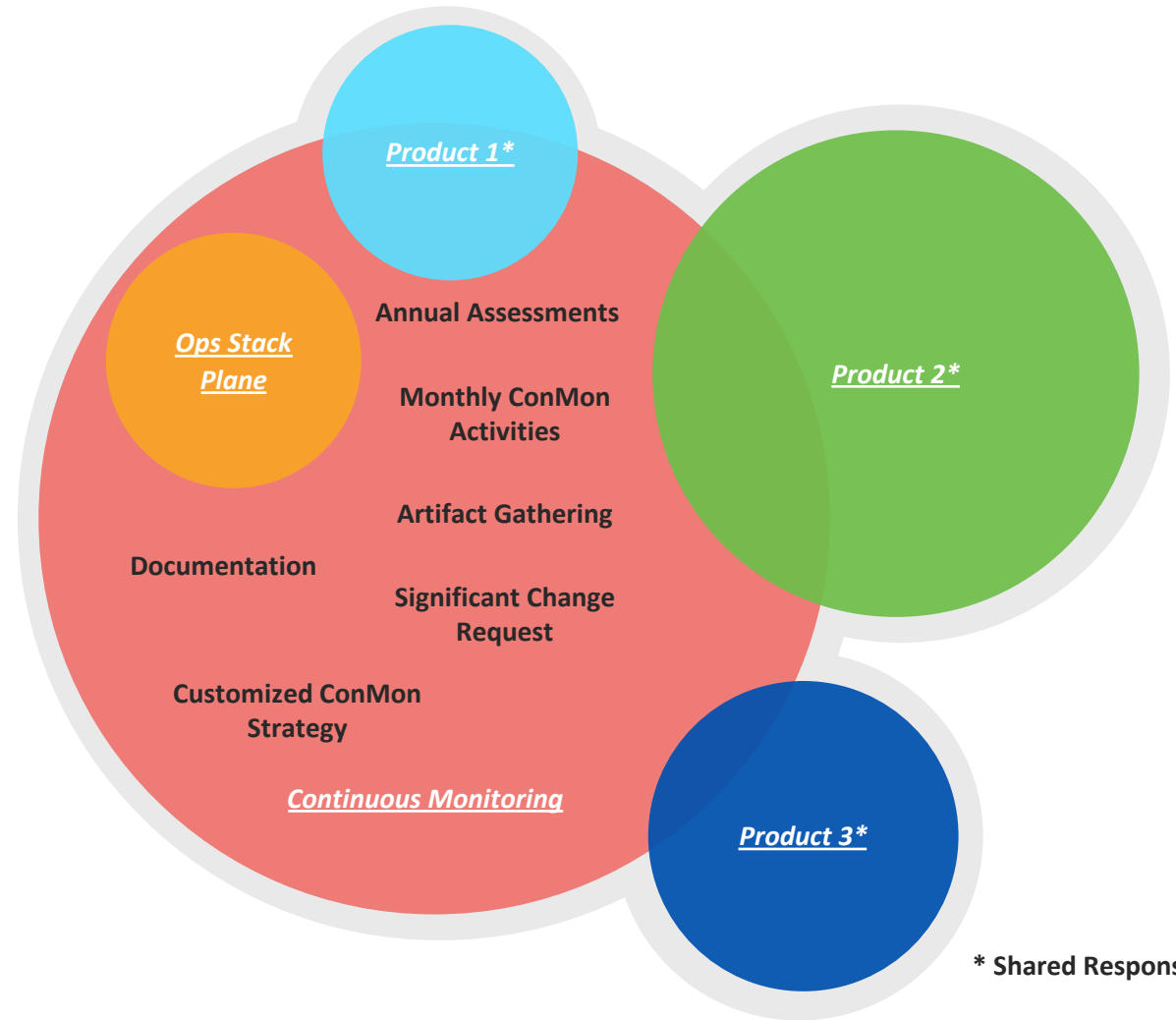
**Baseline SSP creation**

**Evidence collection**

**Documentation**

**Significant Change Requests**

**Change control board advisory support**



\* Shared Responsibility