



A Systems Approach to Software Supply Chain Security and Continuous ATO

Mark Hurter, Solution Architect

29-August, 2022





Agenda

- The AO Dilemma
- Demonstrable Competencies
- Continuous ATO: A New Hope
- Three Layers of Compensating Control
- Q&A
- Closing



OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000



MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Continuous Authorization To Operate (cATO)

The Risk Management Framework (RMF) establishes the continuous management of system cybersecurity risk. Current RMF implementation focuses on obtaining system

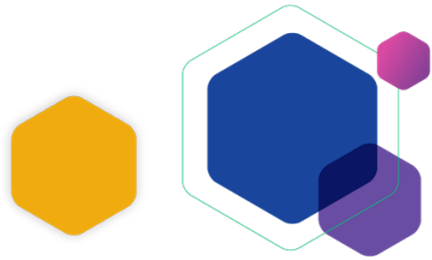
“Current RMF implementation focuses on obtaining system authorizations (ATOs) but falls short in implementing continuous monitoring of risk once authorization has been reached.”

operate under a cATO state.

cATO represents a challenging but necessary enhancement of our cyber risk approach in order to accelerate innovation while outpacing expanding cybersecurity threats. In order to achieve cATO, the Authorizing Official (AO) must be able to demonstrate three main competencies: On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls; the ability to conduct active cyber defense in order to respond to cyber threats in real time; and the adoption and use of an approved DevSecOps reference design.



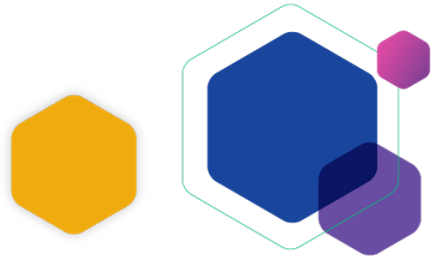
The AO Dilemma



- How do I assess in real time whether or not the application is secure and compliant?
- Based on my risk posture can I assert that I am compliant?
- Do I have the evidence that underpins my assertions?



cATO Demonstrable Capabilities



- The adoption and use of an approved DevSecOps reference design
- On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls;
- Ability to conduct active cyber defense in order to respond to cyber threats in real time





Continuous ATO: A New Hope

- Requirements
 - Continuous == in-process/ ad hoc, on New, and on Change
 - Highly automated
 - Holistic
 - Prioritize fixes
 - Includes compensating controls

Layer 1: The Modeled Reference Design

The screenshot displays a CI/CD pipeline interface with the following stages and tasks:

- Release Readiness** (9 Tasks):
 1. Enable Audit Reports (EC-AuditReports Audit Reports)
 2. Get Jira Tickets (EC-JIRA GetIssues)
 3. Get FE Change Logs (ECSCM-Git CheckoutCode)
 4. Get FE Build Details (EC-Jenkins GetBuildDetails)
 5. Get BE Build Details (EC-Jenkins GetBuildDetails)
 6. Verify Jenkins Build Status (EC-Jenkins GetBuildStatus)
 7. Quality Checks (a. Run Code Quality And Security Scan, b. Run Image Security Scan)
- Quality Assurance (QA)** (4 Tasks):
 1. Deploy to QA (Deployer)
 2. Enable Feature Flag for QA Env (Command)
 3. Send Slack Message (EC-Slack Send Realtime Message)
 4. Run Functional Test (Command)
- Pre-Prod** (1 Entry Gate Rule, 6 Tasks):
 - 1. Wait for Release Manager Approval (Approval)
 - 1. Deploy to Pre-Prod (Deployer)
 - 2. Enable Feature Flag in Pre-Prod (Command)
 - 3. Run SIT Tests (SIT testing)
 - 4. Send Slack message (EC-Slack Send Realtime Message)
 - 5. Verify QA - Notify (Manual)
 - 6. Create ServiceNow ticket (EC-ServiceNow CreateChange Request)
- Exit Gate Rules** (3 Rules):
 1. 100% Passing Pre-Prod Tests (Custom)
 2. No P1s & P2s Issues (Custom)
 3. ATO Approval (Approval)
- Prod** (5 Tasks):
 1. Deploy to Prod (Deployer)
 2. Run smoke tests (Smoke test)
 3. Send Slack message (EC-Slack Send Realtime Message)
 4. Approve final deployment (Manual)
 5. Enable Feature Flag in Prod (Command)

Annotations:

- An arrow points from the "Generate audit reports and build body of evidence for stakeholders & AO." box to the "1. Enable Audit Reports" task in the Release Readiness stage.
- An arrow points from the "Authorizing Official Before application is released to production, analyze evidence before authorization." box to the "3. ATO Approval" rule in the Exit Gate Rules section.

Steps embedded within your CI/CD and release pipelines expedite approvals and ensure continuous authorization worthiness



Common Digital Assets

Code

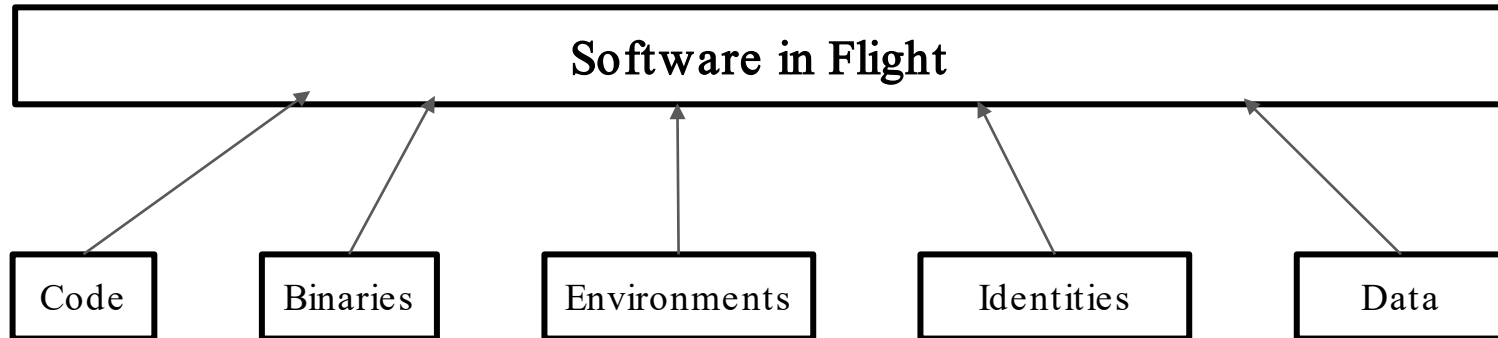
Binaries

Environments

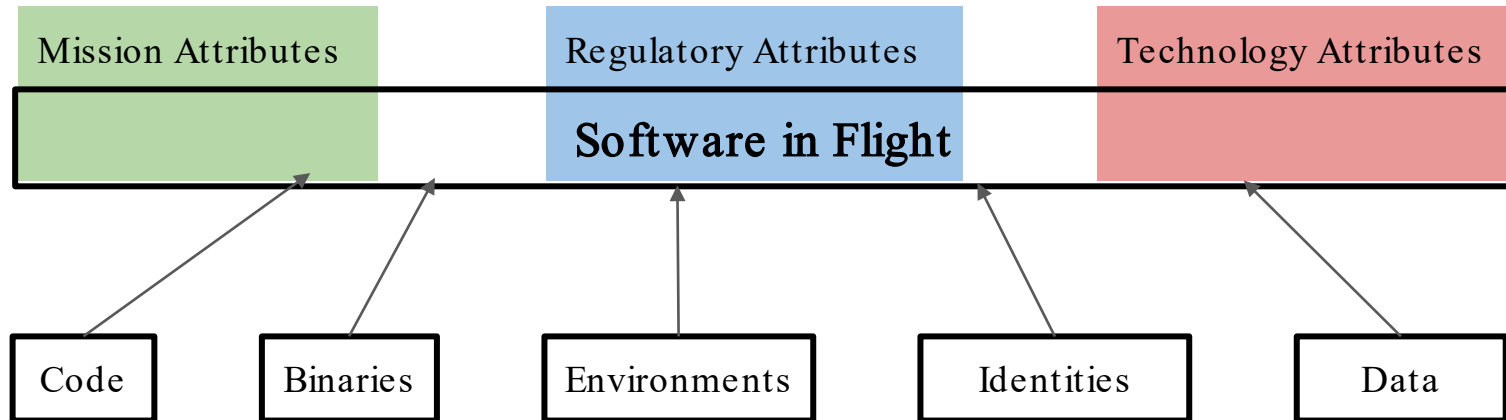
Identities

Data

Define the Application



Model Risk Profile then Select Controls

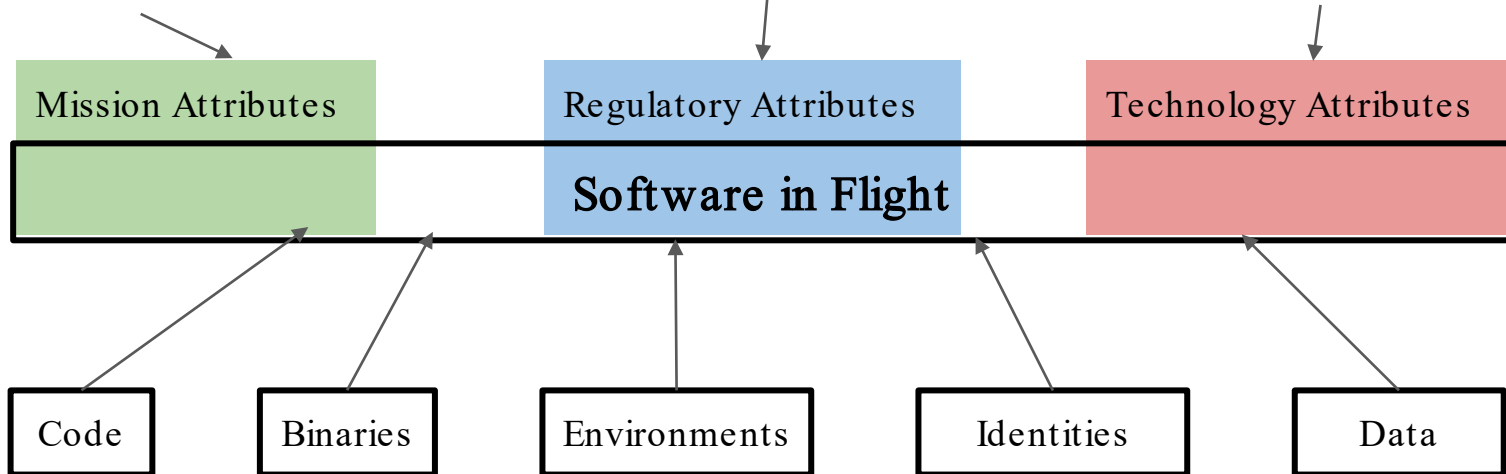


Model Risk Profile then Select Controls

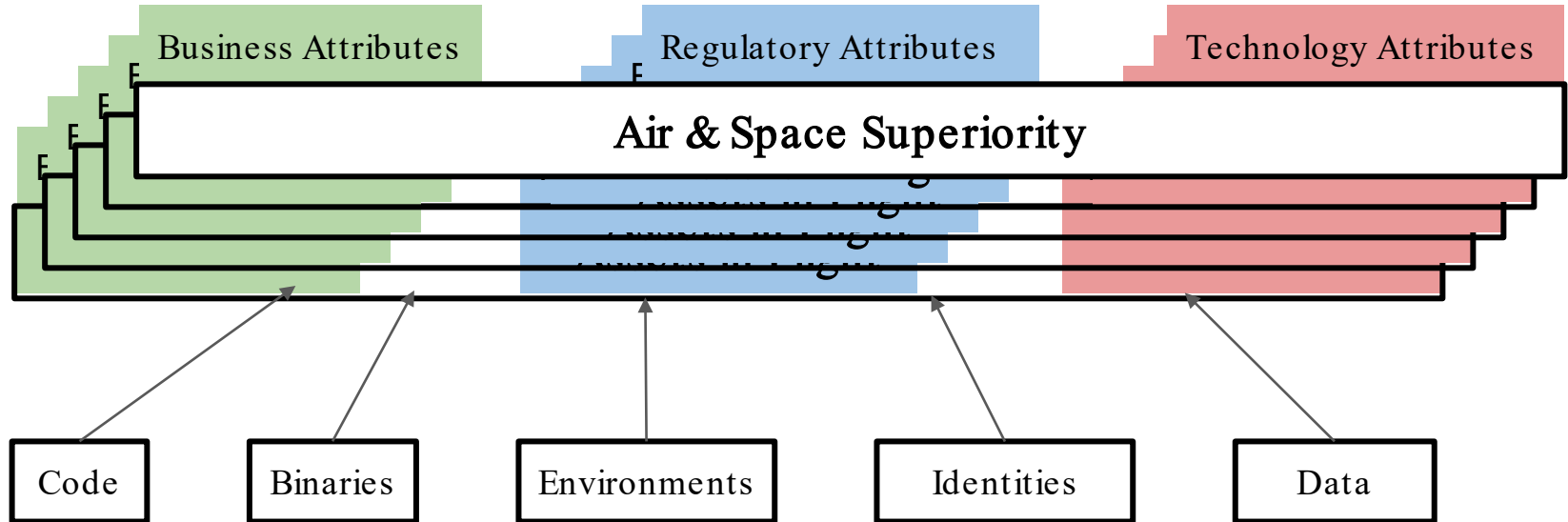
Confidentiality
Integrity
Availability
Data Types

FedRAMP, NIST,
CNSSI

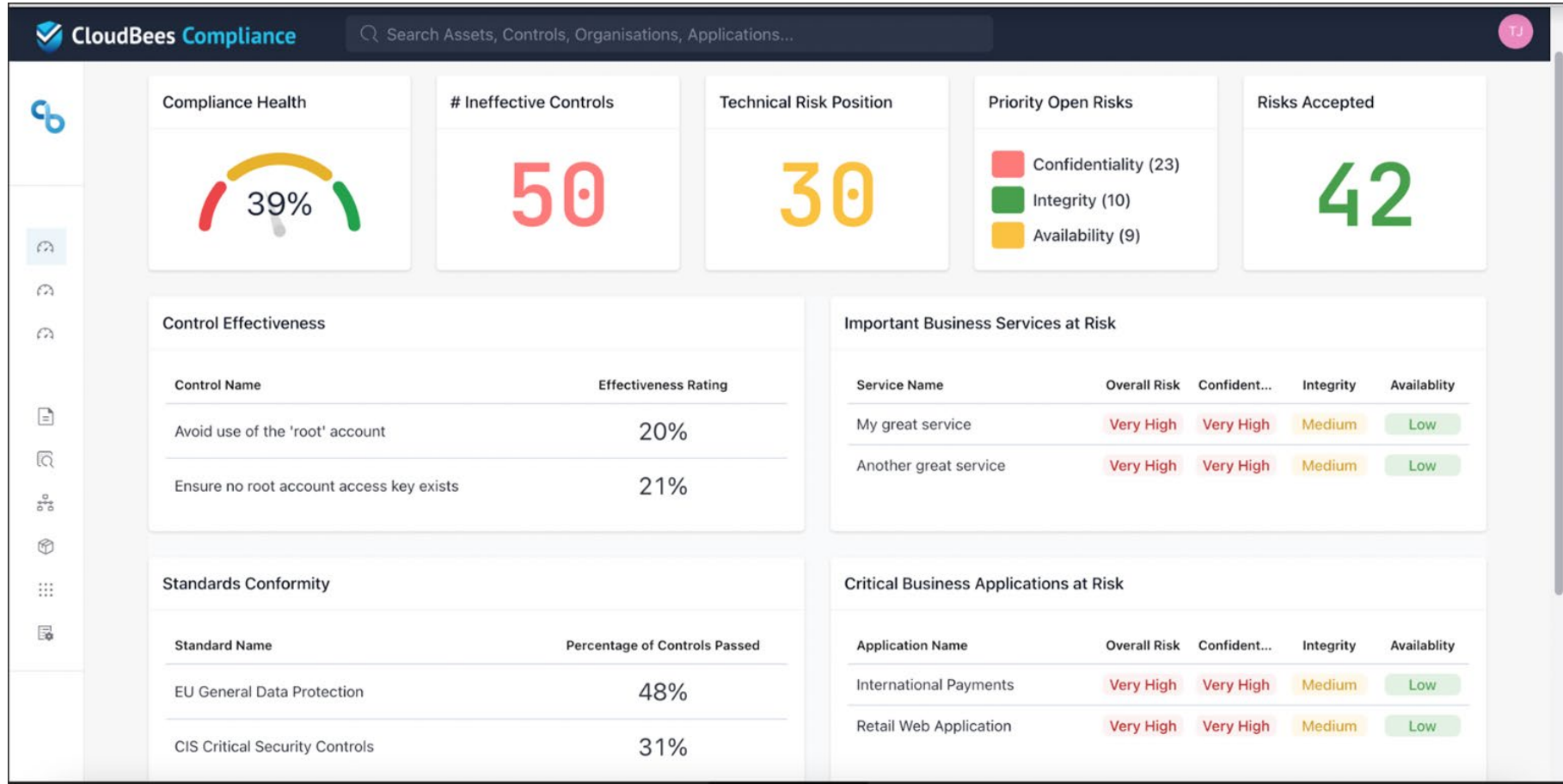
Compatibility
Complexity
Reusability



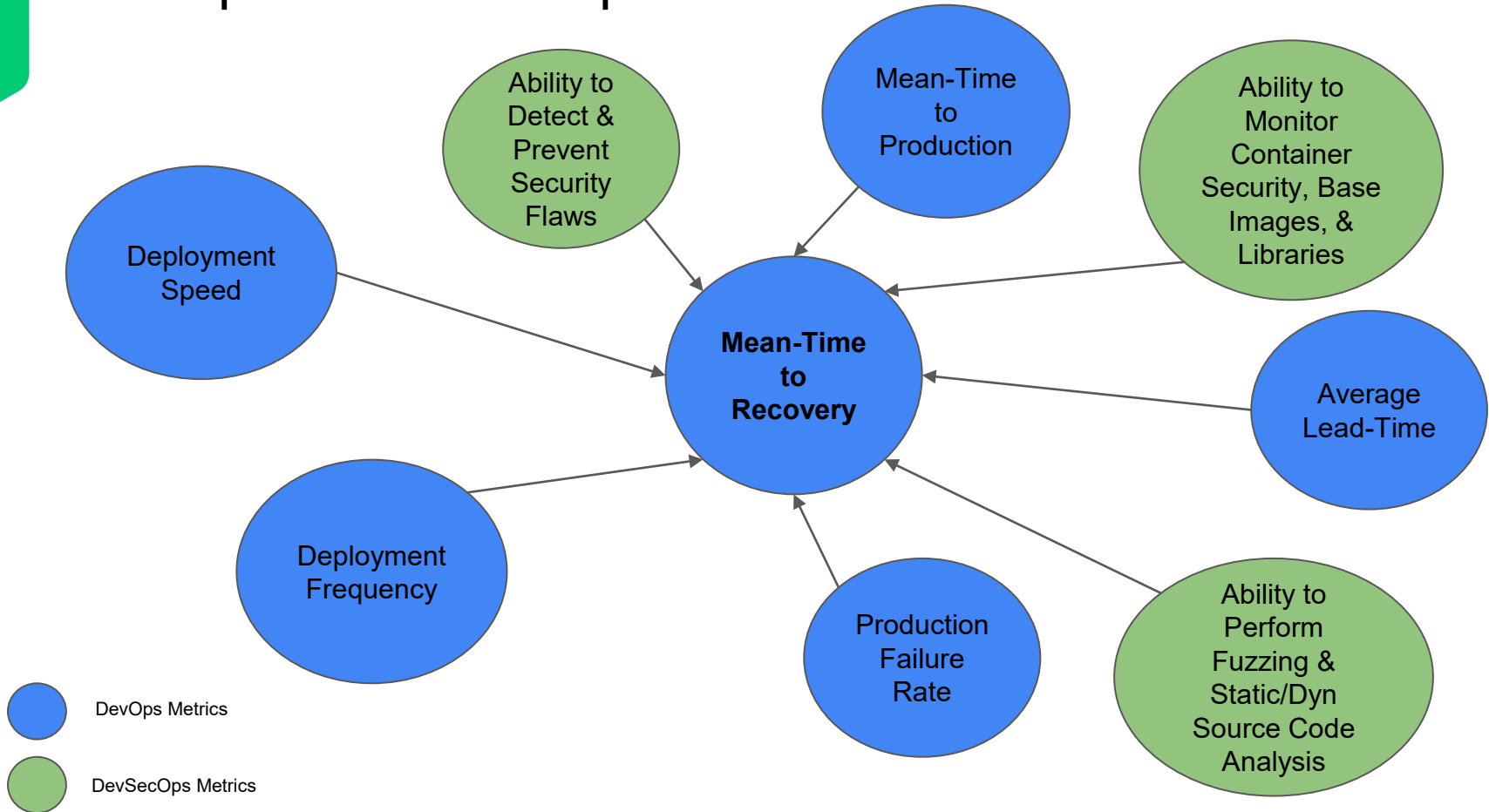
Assemble Applications into Critical Services



Layer 2: On-Going Visibility



DevOps & DevSecOps Metrics





Layer Three: Compensating Controls

Mean Time to Mitigate

- Feature flag as kill switch
 - Everyone has to follow the same build method
 - Kill features, not the experience
- Automated roll back to known good state
 - Rehearsed and integral to the system
 - When a bigger hammer is required

Keys to a Secure Software Supply Chain

Security/Dev Collab

- Security Defines Stds
- Improve Developer Experience
- Increase Velocity
- Improve Risk Posture

Appropriate Tooling

- Low/No Code approach for security
- Consumable by different personas
- Enable rapid response and RT/NRT feedback

Security
Developer
Collaboration

Automate

Appropriate
Tooling

Centralized
Toolsets

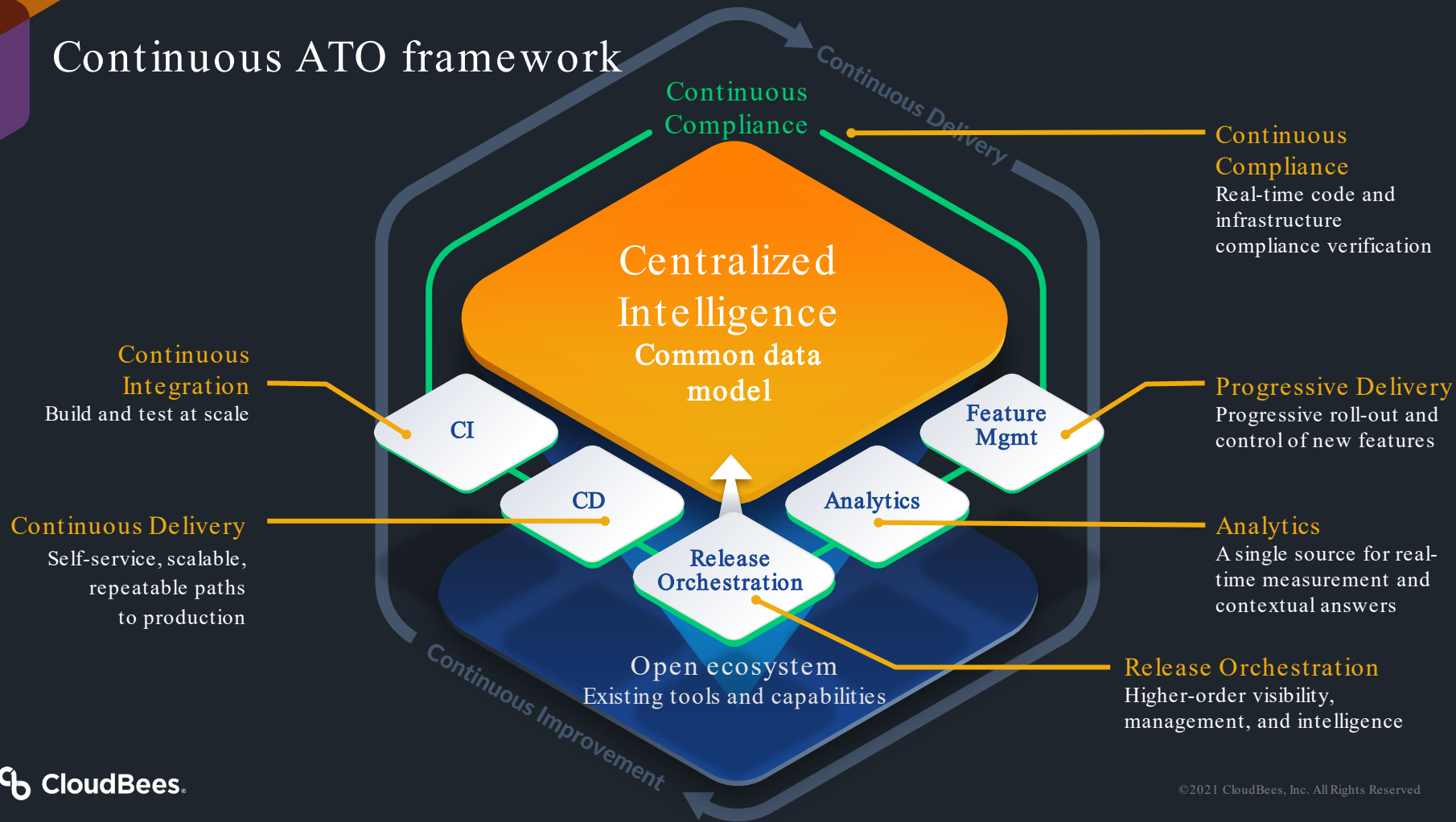
Automate Controls

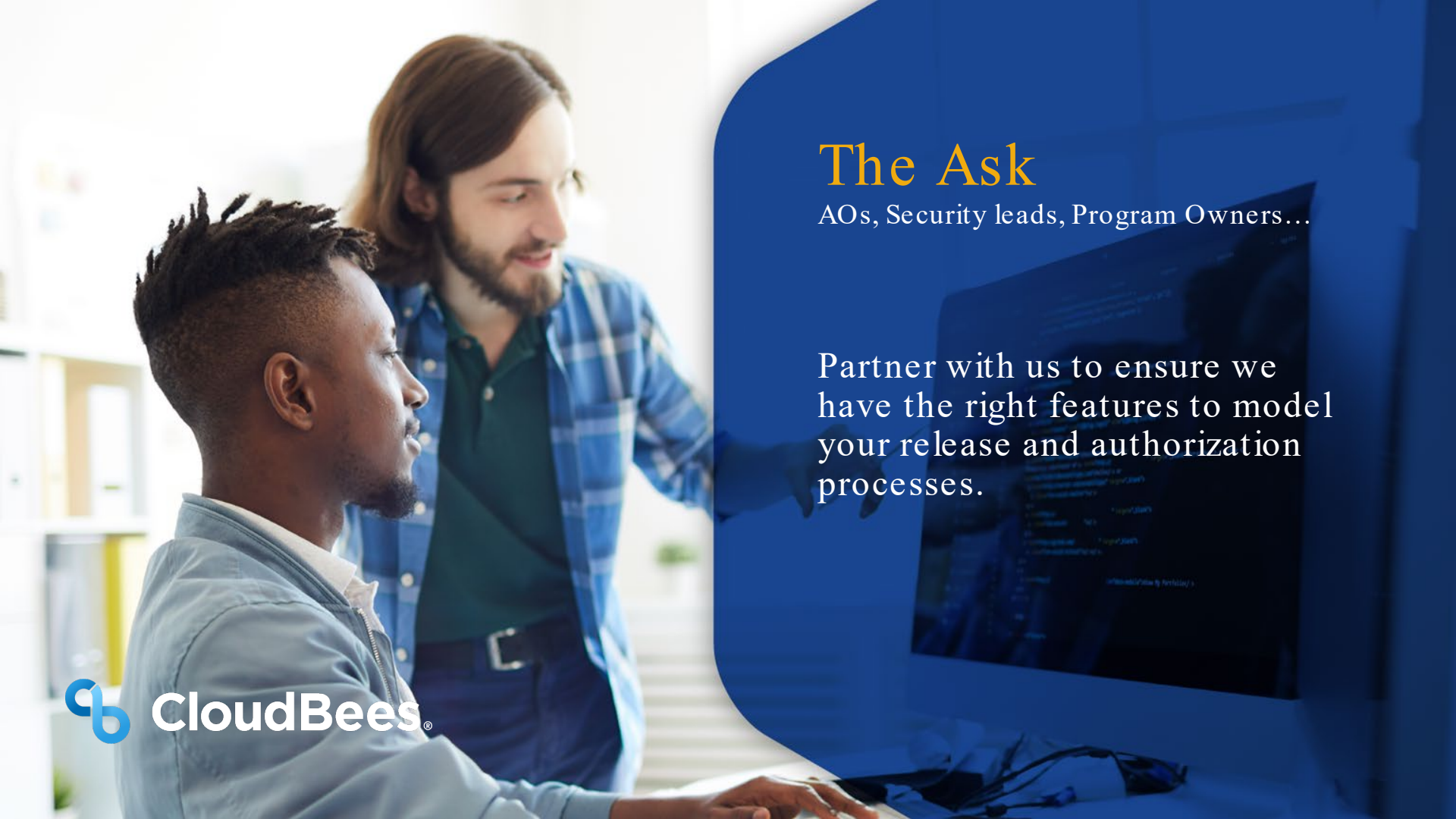
- Continuously Assess
- Evidence as a service
- Control gates prevent non-compliant deployment

Centralized Toolsets

- Enterprise view
- Project view
- Persona-specific dashboards
- Centralized authoritative security/compliance/defect tracking to reduce noise

Continuous ATO framework

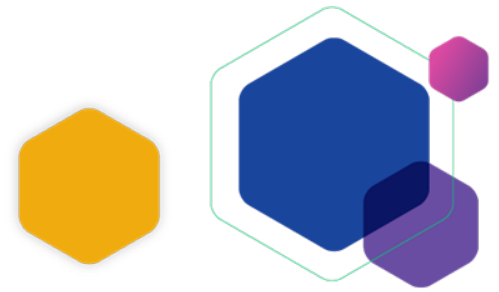


A photograph of two men in an office. One man with dark skin and short dreadlocks is seated, looking at a computer monitor. The other man with light skin and long hair is standing behind him, also looking at the screen. The background is a bright, modern office with shelves. A large blue semi-transparent overlay covers the right side of the image, containing text.

The Ask

AOs, Security leads, Program Owners...

Partner with us to ensure we have the right features to model your release and authorization processes.



Q & A





CloudBees®

<https://www.cloudbees.com/federal>

